Greece's Submission to PACE's Committee on Legal Affairs and Human Rights Request for Information, following Council of Europe's Parliamentary Assembly Resolution 2513 and Report.

March 2024

Executive Summary

Greece shares the concerns of the Parliamentary Assembly of the Council of Europe and all relevant authorities concerning spyware abuses. Accordingly, it has worked closely to provide all the necessary information, conduct parliamentary as well as independent, administrative and criminal investigations, and to take all necessary legislative measures to tighten the legal framework on the use of such software, prohibiting the use and trade, and taking preventive measures to inform and raise awareness in society.

Following the incidents reported in 2022, Greece acknowledged the seriousness of these challenges at the highest political level. An official Parliamentary Inquiry took place to fully examine any allegation and do away with any possible suspicion of use of illegal spyware in official purposes, underlining the independence and trustworthiness of our Institutions. For all the relevant cases and alleged reports of use of surveillance spyware, a comprehensive review conducted by the National Transparency Authority, an independent administrative agency, found no supply or use of illegal spyware by state entities. At the same time, the Data Protection Authority established the use of spyware software by private individuals, informing the citizens whose mobile phone devices were trapped or attempted to be trapped with the particular spyware. In addition, criminal proceedings have been initiated and have been undergoing at the highest level of justice.

Apart from thoroughly investigating the reported incidents, Greece strengthened, improved and further expanded the legal framework in place, making it in one of the most strict and prohibitive legal frameworks in Europe for the use and trade of such malicious spywares, as evident with the Law 5002/2022, 5086/2024 and the strengthening of the Independent Authorities charged with protecting privacy. Law 5002/2022 brought about the immediate prohibition of marketing, possession and use of prohibited tracking software; the establishment of a modern and effective legal framework for waiving the secrecy of communications; the modernization of the action of national intelligence service E.Y.P; the monitoring of the development of new spyware technology. With the new legal framework introduced by L. 5002/2022, a three-member body consisting of two prosecutors and the President of the ADAE decides on informing the affected individuals of any legal surveillance on national security grounds. Therefore, the independence of the process is further strengthened as it is now guaranteed by judicial officials.

In addition, Greece has moved to overall revise and strengthen the functioning of its national security and intelligence authorities, and established a new cybersecurity authority, mandating its cooperation and collaboration with intelligence services and independent data protection authorities, to raise the level of awareness and protection of citizens.

.

Table of Contents

Introduction 4

The Greek Legal Framework in 2022 7

Improvements to the National Legal Framework since 2022 10

A. New legislation on malicious spyware 10

B. Prohibition of the supply for use and trading of illegal spyware and surveillance devices 10

C. Strengthening the checks and balances in surveillance requests & National Intelligence Services 11

Investing towards the prevention of similar incidents 14

Independent Investigations 15

A. Parliamentary Committee Investigation/Inquiry 15

B. Independent Criminal Justice Investigation 15

C. Independent Administrative Investigations 16

Conclusion 17

Appendix 18

Introduction

This submission by Greece to the Committee on Legal Affairs and Human Rights, of the Parliamentary Assembly of the Council of Europe, responds to the request for information by the Rapporteur for follow-up on "*Pegasus and similar spyware and secrete state surveillance*"[1], following Council of Europe's Parliamentary Assembly's Resolution 2513 (2023)[2]. The submission provides all the necessary and relevant information to the Rapporteur's inquiry, in good faith, with due regard and respect to the ongoing criminal justice investigation of allegations of spyware use. The submission recognizes that within the scope of the Rapporteur's report and inquiry falls the use of Pegasus and similar intrusive surveillance software and not any lawful, proportionate and conventional means of surveillance, deployed in the interest of public order and national security[3].

Greece is a country that abides by, upholds and protects the rule of law, not only as a key ingredient for its national public and social order, progress and development, a safeguard for its democracy and prosperity of its people; but also, as the element, the common value and fundamental principle that bides European nations in greater unity, as mentioned in the Statute of the Council of Europe of 1949[4]. Against this backdrop, the Greek Government confirms its adherence to European values, as enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms, and looks forward to cooperating with all the institutions of the Council of Europe, especially the Parliamentary Assembly.

It is recognized, both in Council of Europe's Parliamentary Assembly Resolution 2513 and in the Report of the European Parliament's Committee of Inquiry that the wide-spread trading and use of malicious spyware around the world and in Europe constitutes a common problem, and has affected Greece as much as 13 other countries in Europe and 11 more countries internationally.[5] The concept and need to protect and shield the individual against abuses which may accompany the collection and processing of personal data is not new, and the Council of Europe has been a pioneer in this, with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in

[1] Doc. 15825 -Report-Working document, available at: https://pace.coe.int/en/files/33018/compendium
[2] Resolution 2513 (11/10/2023), available at: https://pace.coe.int/en/files/33116
[3] Paragraph 11.3 (1-4), Resolution 2513 (2023).
[4] Statute of the Council of Europe (ETS 1), London, 5.V.1949, available at: https://rm.coe.int/1680306052
[5] Doc.15825, Report, "Pegasus and similar spyware and secrete state surveillance", Committee on Legal Affairs and Human Rights.

1981[6]. However, the advancement of technology in recent years, undoubtedly, creates new challenges in the protection and integrity of data communication and of data privacy, allowing actors to profit from the use of malicious software, which often provides possibilities that have not been tackled with at regulatory level.

In this context, the competent Greek authorities confirm their will for a full investigation of the factual and legal incidents, referred to in the context of resolution 2513 (2023) of the Parliamentary Assembly of the Council of Europe. Considering the importance given in this case to Article 8 of the ECHR, the Greek Government condemns, unreservedly, the use of illegal monitoring software and has taken drastic measures to protect all residents of Greece against acts that violate their fundamental privacy rights. As Greece shares the concerns of the Parliamentary Assembly of the Council of Europe and all relevant authorities, it has worked closely to provide all the necessary information, conduct independent parliamentary, administrative and criminal investigations, as well as to take all necessary legislative measures to improve the legal framework on the use of such software, prohibiting the use and trade, and taking preventive measures to inform and raise awareness in society. This is well reflected in the European Commissions' Rule of Law Report (2023) chapter for Greece[7], as well as in the European Commissions' reply to European Parliament's Committee on Petitions[8] in the summer of 2023.

A clarification needs to be made, regarding the scope of inquiry of the Rapporteur, as Resolution 2513 recognizes and distinguishes between the actions that a sovereign state must take to safeguard its national security, through proportionate means and actions of national intelligence services, to prevent or investigate a specific act amounting to a genuine and serious threat to national security or a specific and precisely defined serious crime, and, on the other hand, of the rampant use of malicious software by private actors. It is imperative to clarify so much for the Parliamentary Assembly's Report and as much for its Rapporteur and his work, to take note and reflect on the fact that the Greek authorities have not been implicated in illegal surveillances, given that the investigations so far have not found or

[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg 28/01/1981.
[7] 2023 Rule of Law Report Country Chapter on the rule of law situation in Greece, available at: https://commission.europa.eu/document/download/10bc40c8-b6f5-4ad4-8bde-b2ee4df33680_en?filename=21_1_52575_coun_chap_greece_en.pdf
[8] European Parliament, Committee on Petitions, Petition No 0786/2022, Commission Reply 19/6/2023, CM\1281319EN.docx, available at: https://www.europarl.europa.eu/doceo/document/PETI-CM-750025_EN.docx

proven for any public authority or agency to be using illegal malicious software similar to Pegasus.

In particular, Greece, following the incidents reported in 2022, the reports published by various civil society networks, as well as the investigations conducted by all National Independent Authorities, has moved to initiate all available investigations, at the levels of the Hellenic Parliament, independent administrative authorities and one at the level of criminal proceedings. At the same time, we have strengthened, improved and further expanded the legal framework in place, making it one of the most strict and prohibitive legal frameworks in Europe for the use and trade of malicious spywares. In addition, we have moved to establish a separate cybersecurity authority and a cyber security coordination committee, ensuring their cooperation and collaboration with intelligence services and independent data protection authorities, to raise the level of awareness and protection of citizens.

The Greek Legal Framework in 2022

Greek Law offers a wide range of rights both for the protection of communication privacy and for the protection of personal data. The Greek Constitution, in Article 9.a states that "*Everyone has the right to protection from the collection, processing and use, especially by electronic means, of their personal data, as defined by law. The protection of personal data is ensured by an independent authority, which is established and operates as prescribed by law*"[9].

What is more, Article 19 of the Constitution states that,

> "*1. The privacy of letters and the freedom to respond or communicate in any other way is absolutely inviolable. The law defines the guarantees under which the judicial authority is not bound by confidentiality for reasons of national security or to investigate particularly serious crimes. 2. Law defines the matters related to the formation, operation and responsibilities of an independent authority that ensures the confidentiality of paragraph 1. 3. The use of evidence obtained in violation of this article and articles 9 and 9A is prohibited*".

Importantly, the protection of privacy was elevated to a constitutional provision as early as the Constitution of 1844. In fact, it resulted in the establishment of the judicial review of constitutionality of legislation in Greece with the historic decision of Greece's Supreme Court (Areios Pagos) 169/1893.

In modern times, the protection of privacy concerns not only written messages (letters), but also any form of private, *i.e.* non-public communication, such as telegrams, telephone calls, facsimile messages, electronic messages (e-mails), which are the modern form of letters. Confidentiality is lifted according to the conditions set by the constitutional provision itself[10]. In this context, two independent authorities are foreseen at the national level: The Hellenic Data Protection Authority (HDPA) and the Authority for Ensuring Privacy of Communications (ADAE) respectively.

---

[9] The Constitution of Greece, as revised in November 2019, available in its latest version at: https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/THE%20CONSTITUTION%20OF%20GREECE.pdf

[10] Plenary, Supreme Court Decision, AP 1/2017, available at: https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=FBQ53ZVG8NUXT8DR98J2C86I6LQ4NJ&apof=1_2017&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%CF%CB%CF%CC%C5%CB%C5%C9%C1#

The **Hellenic Data Protection Authority** (HDPA) is a constitutionally protected Independent Public Authority established by Law 2472/1997[11], which incorporated into Greek law the European Directive 95/46/EC for the protection of natural persons against the processing of personal data and for the free movement of such data[12]. Now, as of 29/8/2019, law 4624/2019 is in effect ("*Principle for the Protection of Personal Data"*, implementing measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, for the protection of natural persons against the processing of personal data and incorporation into national legislation of Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 and other provisions).

In the aforementioned law (4624/2019), articles 9 to 20 refer to the Hellenic Data Protection Authority, as supervisory authority. Law 4624/2019 also includes the incorporation into the Greek legal order of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons against the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions and for the free movement of such data and the repeal of Council Framework Decision 2008/977/JHA[13]. Also, with regard to the protection of personal data in the field of electronic communications, the Authority applies the law 3471/2006 which respectively incorporates into the national law the European Directive 2002/58/EC[14].

The **Authority for Ensuring Privacy of Communications** (ADAE) aims to protect the privacy of letters, the free response or communication in any other way as well as the security of networks and information and was established by Article 1 of Law 3115/2003, in accordance with paragraph 2 of article 19 of the Constitution. The concept of protecting the confidentiality of communications also includes the control of compliance with the conditions and the procedure for lifting confidentiality, provided for by law. ADAE is an Independent

[11] Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended), available at: https://www.dpa.gr/sites/default/files/2019-10/law_2472-97-nov2013-en.pdf

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

[13] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058

Authority that enjoys administrative autonomy. ADAE is subject to parliamentary control in the manner and procedure each time provided for by the Parliament's Rules of Procedure.

In accordance with article 6 of L. 3115/2003, ADAE has the power to conduct audits of installations, equipment, archives, data bases and documents of the Hellenic National Intelligence Service (E.Y.P.), of other public authorities, as well as of private corporations that engage in postal, telecommunications, or other services concerning networking and communications; it summons hearings of public officials and individuals; it proceeds to the seizure of means of confidentiality violations and to the destruction of information, evidence or data, which were obtained illegally; it examines complaints regarding the protection of the applicants' rights concerning their rights to communication privacy.

The use of Pegasus and similar spyware was not allowed in Greece at the time of the reported incidents in 2022. However, a reassessment of the existing legal framework necessitated a number of improvements that were subsequently enacted to close potential loopholes and more fully and comprehensively protect the privacy of communications.

Improvements to the National Legal Framework since 2022

A. New legislation on malicious spyware

Greece was one of the Member States of the Council of Europe that malicious software and actors that profit in their trade and use for personal gains became active. Similarly, countries such as Spain, Belgium, France and others, were also examples where malicious software managed to infiltrate and disseminate. There are many cases in which officials, private individuals and companies were targeted, as a result of the gap that exists in the technological advancement and possibilities made in the field of spyware and intrusive malware one the one hand and the knowledge and reflexes authorities, private actors and the justice can demonstrate on the other.

Nonetheless, upon becoming aware of the use of illegal tracking software, the Greek authorities, finding deficiencies in the existing legal framework, took immediate measures to correct institutional deficiencies. With Law 5002/2022 "*Procedure for lifting the confidentiality of communications, cyber security and protection of citizens' personal data*" (Government Gazette A 228/9.12.2022)[15], Greece acquired one of the strictest regulatory frameworks in Europe regarding the protection of privacy in communications. In addition, before the passing of the bill, both the competent EU Commissioner and the PEGA committee of the European Parliament were informed.

In overview, the new law achieves:

1. The criminal horizontal prohibition of marketing, possession and use of prohibited tracking software and surveillance devices.
2. The establishment of a modern and effective legal framework for waiving the privacy of communications.
3. The strengthening of the transparency and efficiency in the functioning of the national intelligence service (E.Y.P.).

B. Prohibition of the supply for use and trading of illegal spyware and surveillance devices

In more detail, and in relation to malicious surveillance software like Pegasus, Chapter C of L. 5002/2022 (articles 10-14) significantly enhances the criminal protection of

[15] Law NUMBER 5002 (GAZETTE A' 228/09-12-2022), Procedure for lifting the confidentiality of communications, cyber security, and protection of citizens' personal data, available in Greek: www.et.gr.

communications privacy, specifically targeting spyware. In particular, Articles 10 and 11 of L. 5002/2022 upgrade from misdemeanors to felonies Articles 370A and 370E of the Criminal Code respectively, regarding violation of privacy of telephone and oral communication as well as violation of non-public transmissions of data or electromagnetic emissions.

Most importantly, in a significant novelty, Article 12 of L. 5002/2022 introduces a new article in the Criminal Code (370F), horizontally prohibiting the circulation of monitoring software and devices. According to this provision, *"whoever produces, sells, procures for use, imports, exports, owns, distributes or otherwise traffics software or tracking devices, with the possibility of interception, recording and any kind of extraction content or communication data (motion and location)*" so as to violate the privacy of telephone communication, faces criminal sanctions, that is imprisonment of at least two years.

Law 5002/2022 also allows state entities to procure surveillance software or devices only under the conditions set out in a presidential decree (article 13); that is, under the conditions preemptively (*ex ante*) approved by the Council of State, Greece's Supreme Administrative Court. Currently, the draft presidential decree is in the process of being finalized and will be submitted to the Council of State in April 2024. In addition, according to the law, ADAE issues (and updates on a regular basis) an indicative list of software or monitoring devices, that is publicly available along with appropriate protection measures (article 14 L. 5002/2022). This constitutes a direct provision for the prevention of similar incidents, for the protection and information of individuals, as it raises the level of awareness on malicious surveillance software and provides information to protect oneself, as well as file complaints with the competent authorities and seek redress from justice.

C. Strengthening the checks and balances in surveillance requests & National Intelligence Services

What is more, given the seriousness of the alleged cases and the implications for fundamental rights, Greece did not limit herself to stricter provisions for malicious surveillance software, but took further steps to improve and strengthen the way that national intelligence services function.

Emergency legislation (*Πράξη Νομοθετικού Περιεχομένου*) enacted in August 2022 included a set of first steps to increase integrity in the operation of the country's intelligence services (E.Y.P.): It introduced a parliamentary hearing prior to the appointment of E.Y.P.

Governor and it reestablished the rule that two judicial officers need to approve lifting the secrecy of communications, if so requested by E.Y.P.

Less than four months later, Law 5002/2022 brought about broader changes in the way E.Y.P. operates, so that its action becomes more rational and its organization is improved by establishing the necessary service units for its more effective action and enhancing transparency during its operation. Article 15 established an Internal Audit Unit in E.Y.P., whereas article 18 introduced specific qualifications for the appointment of the E.Y.P. Head and article 19 introduced within E.Y.P. an Intelligence and Counterintelligence Academy.

At the same time, Law 5002/2022 established stronger safeguards for waiving the secrecy of communications. Consistent with Article 19 of the Constitution, Articles 4 and 6 of Law 5002/2022 provide for a strict waiving procedure only for reasons of national security or for the investigation of specific restrictively mentioned, serious crimes.

For reasons of national security, the secrecy of communications can be waived only by E.Y.P. or by the Hellenic Police's Counterterrorism Unit (*Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας*). For the first time, the 2022 legislation included a definition of "national security", including reasons that relate with the protection of the state's basic functions and the citizens' fundamental interests, such as national defense, foreign policy, energy security and cyber-security (article 3 of L. 5002/2022). Provided that these requirements are met, two public prosecutors - judicial officers who enjoy full independence according to the Constitution – need to approve waiving the secrecy of communications. In a further novelty of the 2022 legislation, if political figures (as listed in article 3 of L. 5002/2022[16]) are implicated, additional safety clauses are provided: Due to the special importance of the act and to preserve the functioning of the democratic state, the Speaker of the Parliament needs to also approve of waiving the secrecy of communications and only E.Y.P. is entrusted with submitting a request for waiving the secrecy of communications, based on specific evidence that demonstrates an immediate and highly probable risk to national security. In addition, the 2022 legislation for the first time in Greece introduced an individual right to be informed regarding any waiving of communications secrecy on national security grounds provided that (a) the purpose for the waiving is not compromised and (b) three years have elapsed, based upon the assessment of a three-member body comprising of two judicial officers and the ADAE President (article 4 par. 7 L. 5002/2022).

[16] The list includes the President of the Republic, members of the government and deputy ministers, members of the national and European parliaments, leaders of the political parties represented in the national and European parliaments and the heads of municipalities and regions.

For the investigation of crimes, the secrecy of communications can be waived only for particularly serious crimes, with a strong social stigma. To more comprehensively protect the privacy of communication, the 2022 legislation considerably reduced the number of crimes that might justify such an extraordinary measure, provided that a judicial board made up of judicial officers grants the relevant permission. In this case as well, after the expiration of the measure and upon submission of a relevant request by the affected party, ADAE notifies her of the imposition of this measure within a period of sixty (60) days, with the consent of the Supreme Court Prosecutor and under the condition that the purpose for which the measure was ordered is not compromised (article 6 L. 5002/2022).

Against this backdrop, Greek legislation is currently at the forefront of international and European developments. To fully protect privacy of communications against ever increasing threats and challenges, a comprehensive legal framework is in place including criminal sanctions against privacy violations; clearly delineated circumstances and procedures for legally waiving the secrecy of communications; awareness measures and transparency guarantees.

Prevention of similar incidents

At the same time, with the same law 5002/2022, an effort was undertaken to prevent new cyber security breach phenomena. Initially, this law provided for the coordination of all national authorities that have a point of reference in cyber security by a newly established cyber security coordination committee. The aim of this reform is to better deal with cyber-attacks for the future. The Coordinating Committee for Cyber Security issues as defined in article 20 et seq. of Law 5002/2022, has as its mission the planning, monitoring, coordination of actions, interventions in issues related to cyber security from the initial stage of prevention to the stage of effectively dealing with cyber-attack incidents and minimizing the impact of cyber threats.

What is important and crucial here in the role of the Cybersecurity Committee is its interaction, cooperation and coordination with the competent authorities in providing information on the list of illegal malicious software or devices for surveillance. In particular, the Committee makes recommendations to the Independent Authority for Securing Communications (ADAE) on the list of all malicious surveillance software or devices.

In addition to the Cyber Security Committee, and in the overall context of enhancing the privacy and cyber security at a national level, further cyber security measures were put at the center of the recent law 5086/2024 "*National Cyber Security Authority and other provisions*" (Official Gazette A' 23/14.02.2024). This law provides for the organization of an operational system related to cyber security, through the modernization and strengthening of the capabilities of the competent National Cyber Security Authority, which becomes a legal entity under public law (N.P.D.D.), in order to become more efficient in the performance of its duties. At the same time, it aims to maintain and strengthen citizens' trust in digital services, through the definition of a transparent framework of roles, responsibilities and accountability for the confidentiality, availability and data integrity of critical digital systems (article 1 L. 5086/2024).

Independent Investigations

A. Parliamentary Committee Investigation/Inquiry

In the echo of the allegations regarding the use of surveillance software in Greece, the Hellenic Parliament intensively investigated all related reports. In the first place, the Institutions and Transparency Committee, inter alia responsible for parliamentary control of independent authorities and the national intelligence service (according to article 43 A of the Parliament's Standing Orders), dealt with the issue in lengthy sessions in July and September 2022, also with the participation of key witnesses; the Parliament additionally established, in August 2022, an Official Committee of Inquiry (consistent with article 68 par. 2 of the Constitution and article 144 of the Parliament's Standing Orders) with the participation of all parliamentary factions and independent members of Parliament. Importantly, making use of a significant novelty enacted in the 2019 constitutional amendments, the Committee was established upon request submitted by the parliamentary opposition.

Respecting the sensitive information pertaining to national security, the Committee conducted its inquiry under confidentiality, allowing all members to assess and investigate all relevant material, including calling witnesses. The Committee examined how the national intelligence services, in their role, might be conducting legally authorized surveillance operations, through proportionate and conventional means. The Committee's sessions lasted almost 60 hours while their detailed minutes number some 3.000 pages.

The findings of the Committee (222 pages) were made available, under confidentiality, to all Members of the Hellenic Parliament, and a debate on the findings was held in December 2022, at the Plenary Session of the Hellenic Parliament.

B. Independent Criminal Justice Investigation

As far as the criminal part of the case is concerned, a criminal investigation is ongoing. While the relevant investigation was initially carried out by the Athens First Instance Prosecutor's Office, due to its importance it was upgraded to the highest level and is now carried out by the Supreme Court Prosecutor's Office, in order to ensure full investigation of the case. It should be noted that the competent judicial authorities act completely independent in the exercise of their duties, given the strong separation of powers established in the Greek Constitution.

C. Independent Administrative Investigations

All competent national independent authorities performed separate and independent investigations, with regard to these incidents:

The **Independent Authority for Securing Communications (ADAE)**, tasked with the protection of free correspondence and communications, conducted intensive and thorough investigations regarding the alleged violations, collected evidence, held hearings and formed a special task force to this purpose[17].

The **Hellenic Data Protection Authority (HDPA)**, tasked with the the protection of individuals with regard to the processing of personal data, also conducted a thorough investigation on the matter, formed a special task force, collected evidence from all parties involved[18].

The **National Transparency Authority (NTA)**, tasked with safeguarding transparency and integrity as well as combatting corruption, performed an investigation of its own on the allegations regarding malicious spyware.

The results of the concluded investigations have reached no conclusion or indication that national authorities were involved in the use of illegal surveillance software, while there are certain investigations still ongoing.

[17] See 2022 Annual Report from ADAE, Chapter 2, section 1.3, pages 44-45, and section 5.5.b, page 81, available (in Greek) at: file:///C:/Users/gplevris/Downloads/EP_ADAE_2022.pdf

[18] See Press Release from HDPA, dated July 20th, 2023 regarding actions taken by the Independ Authority vis-à-vis the use of malicious spyware in Greece, available (in Greek) at: https://www.dpa.gr/el/enimerwtiko/deltia/energeies-tis-arhis-se-shesi-me-drastiriotites-egkatastasis-kai-hrisis

Conclusion

The possibilities and malicious uses that arise from the advancements in technology and software development in relations to privacy and data protection constitute a serious challenge for Europe and for all democratic countries. Given the constant and fast-paced technological advances, we must remain vigilant and raise the level of awareness in our societies, as well as cultivate the technological and cybersecurity means to address them.

Greece, as many other member states of the Council of Europe, found herself faced with such challenges in 2022. The existing -at the time- legal framework was not sufficiently positioned to tackle the effects of such intrusive surveillance software and their advance capabilities. Since then, we have taken all the necessary steps at the legislative level to create such a legal ecosystem that would prohibit and deter from the supply for use and trading of surveillance software, as evident with the Laws 5002/2022, 5086/2024 and the strengthening of the Independent Authorities tasked with protecting privacy and data.

Greece, also, acknowledged the seriousness of this challenges at the highest political level. Notwithstanding the legitimate, necessary and crucial to national security, role of the intelligence services community, we proceeded with improving and strengthening their framework of operation.

What is more, an official Parliamentary Inquiry and all possible administrative proceedings have taken place to fully examine any allegation and do away with any possible suspicion of use of such software in official purposes, underlining the independence and trustworthiness of our Institutions. For all the relevant cases and alleged reports of use of surveillance spyware, criminal proceedings have been initiated, and have been undergoing at the highest level of justice.

Appendix

LAW UNDER NUMBER 5002

GOVERNMENT GAZETTE A 228/9.12.2022

Procedure for lifting the confidentiality of communications, cyber security, and protection of citizens' personal data.

THE PRESIDENT OF THE HELLENIC REPUBLIC

We hereby issue the following law passed by the Parliament:

CONTENTS

Chapter A: General provisions

Article 1 Purpose

Article 2 Subject

Article 3 Definitions

Chapter B: Lift of communication confidentiality

Article 4 Lift of communication confidentiality for reasons of national security

Article 5 Management of material in lifts for reasons of national security

Article 6 Lift of communication confidentiality for the detection of crimes

Article 7 Management of material in lifts for the detection of crimes

Article 8 Procedure for lifting confidentiality

Article 9 Judicial officers of the Hellenic Police and the Hellenic Coast Guard. Modification of para. 3 of article 5 of law 3649/2008 and para. 3 of article 4 of law 2265/1994

Chapter C: Surveillance software

Article 10 Violation of telephone communication and oral conversation confidentiality. Amendment of article 370A of the Penal Code

Article 11 Violation of non-public data transfers or electromagnetic emissions. Amendment of article 370E of the Penal Code

Article 12 Prohibition of circulation of surveillance software, devices, and other data. Addition of article 370ST to the Penal Code

Article 13 Supply of software and surveillance devices by the State

Article 14 Information on surveillance software or devices

Chapter D: Hellenic Police Issues

Article 15 Structure of the Hellenic Police. Amendment of para. 4 of article 3 of law 3649/2008

Article 16 Operation of the Center for Technological Support, Development, and Innovation (CETUDI) and enhancement of transparency. Amendment of para. 2 of article 3A of law 3649/2008 and para. 5 of article 38 of law 4412/2016

Article 17 Information Security Authority (INFOSEC) issues. Amendment of para. 7 of article 4 of law 3649/2008

Article 18 Administration of the Hellenic Police. Amendment of para. 2 and replacement of para. 4 of article 9 of law 3649/2008

Article 19 Information and Espionage Police Academy. Amendment of para. 1 of article 13 of law 3649/2008

Chapter E: Cybersecurity Issues

Article 20 Establishment of a Coordination Committee for Cybersecurity Issues

Article 21 Committee's Mission

Article 22 Committee's Powers

Article 23 Establishment and operation of the Committee

Article 24 Committee's Working Groups

Article 25 Committee's Administrative Support

Article 26 Obligation of information and assistance provision

Article 27 Support of actions of the national coordination center. Amendment of para. 2 of article 17 of law 4961/2022

Article 28 Monitoring of threats and vulnerabilities of information and communication systems

Article 29 National Risk Assessment Plan of Information Technology and Communication Systems

Article 30 Staffing of the National Cybersecurity Authority (NCA). Amendment of para. 5 of article 50 of law 4635/2019

Article 31 Unified Security Operations Center (SOC) Establishment of a National SOC Network

Article 32 Authorizing provisions for cybersecurity issues. Addition of article 14A to law 4577/2018
Article 33 Expansion of the scope to other entities. Addition of article 14B to law 4577/2018

Chapter F: Personal Data Protection
Article 34 Definition of the Data Protection Officer in public bodies. Replacement of para. 5 of article 6 of law 4624/2019
Article 35 Scope of law 4624/2019. Replacement of article 43 of law 4624/2019
Article 36 Definitions. Amendment of articles 44, 53, 58, and 71 of law 4624/2019
Article 37 Replacement of the title of Part II of Chapter D of law 4624/2019
Article 38 Legitimacy of processing. Addition of article 45A to law 4624/2019 (article 8 of Directive 2016/680)
Article 39 Processing of special categories of personal data. Replacement of article 46 of law 4624/2019
Article 40 Processing for other purposes. Amendment of article 47 of law 4624/2019
Article 41 Subject's consent. Replacement of article 49 of law 4624/2019
Article 42 Automated individual decision-making. Replacement of article 52 of law 4624/2019
Article 43 Correction of personal data. Storage and review deadlines. Restriction of processing. Replacement of article 73 of law 4624/2019
Article 44 Repealed provisions. Replacement of article 84 of law 4624/2019
Article 45 Disclosure of personal data by the prosecution. Addition of article 84A to law 4624/2019
Article 46 Establishment of a Permanent Scientific Committee on Personal Data

Chapter G: Authorizing, final, transitional, and repealed provisions
Article 47 Authorizing provisions
Article 48 Final provisions
Article 49 Transitional provisions
Article 50 Repealed provisions

Chapter H: Entry into force
Article 51 Entry into force

CHAPTER A: GENERAL PROVISIONS

Article 1

Purpose

The purpose of this is:

a) to strengthen and modernize the procedure for lifting the confidentiality of communications in accordance with the second paragraph of Article 19 of the Constitution,

b) to optimize the action of the National Intelligence Service,

c) to protect the confidentiality of communications from surveillance software,

d) the organic and functional upgrading of the level of cybersecurity in the country, and

e) more effective protection of natural persons against the processing of personal data.

Article 2

Subject

The subject of this is:

a) the comprehensive regulation of the procedure for lifting the confidentiality of communications,

b) the introduction of amendments to the structure and operation of the National Intelligence Service,

c) the criminal penalty for the trade, possession, and use of surveillance software,

d) the establishment and operation of a Coordination Committee for Cybersecurity issues, and

e) the amendment of the regulations for integration into the national legal order of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA (L 119).

Article 3

Definitions

For the purposes of this:

a) "Reasons of national security" are reasons related to the protection of the basic functions of the state and the fundamental interests of Greek citizens, such as, in particular, reasons related to national defense, foreign policy, energy security, and cybersecurity.

b) "Political figures" are the President of the Republic, members of the government and deputy ministers, members of parliament and members of the European Parliament, the leaders of

political parties represented in the Parliament and the European Parliament, and the supreme solitary bodies of the Regional Authorities of first and second degree.

CHAPTER B: REMOVING PRIVACY OF COMMUNICATIONS

Article 4

Declassification of communications for reasons of national security

1. A request to declassify communications for reasons of national security can only be submitted by the National Intelligence Service (NIS) or the Special Violent Crimes Directorate of the Hellenic Police (D.A.E.E.B.) either on their own initiative or following relevant information transmitted by a judicial or other political, military or police public authority, under whose jurisdiction is the matter of national security that requires the removal.

2. The request for declassification of communications for reasons of national security is submitted, on a case-by-case basis, for the E.Y.P. to the public prosecutor of par. 3 of article 5 of Law 3649/2008 (A' 39), and for D.A.E.E.B. to the prosecuting officer of par. 3 of article 4 of Law 2265/1994 (A΄ 209). The request shall include (a) the reasons constituting a risk to national security, (b) the necessity of declassification to address the risk, (c) the means of response or communication for which declassification is requested, (d) the object of the removal, i.e. the external elements of the communication or its content, and (e) the territorial extent of application and the absolutely necessary time duration of the removal. The public prosecutor shall decide within twenty-four (24) hours on whether or not to lift the confidentiality by his order, which contains the information referred to in paragraphs 4 and 5 hereof. If, in his judgment, after a recommendation from the requesting authority, special circumstances of national security require the omission or brief citation of some of these elements, a special mention is made in the provision. The approval order is submitted without delay, together with the request and the accompanying data brought to the attention of the public prosecutor, for approval to a second public prosecutor, who is a deputy prosecutor of the Supreme Court or a prosecutor of Appeals and is appointed by decision of the Prosecutor of the Supreme Court for a term of office one (1) year, renewable for one (1) year. With a similar decision, the legal deputy of the second prosecutor of the fifth paragraph is also defined. The second prosecutor approves or rejects the request within twenty-four (24) hours and promptly returns all of the above documents to the sender, without the possibility of keeping a record. The validity of the prosecutor's order begins with the approval of the second prosecutor's officer.

As amended by Article 26 LAW 5067/2023 effective 11/21/2023

3. The request for declassification of communications for reasons of national security, concerning political persons, is submitted only by the E.Y.P. and must be based on specific elements that make the jeopardy of national security immediate and highly probable. The request, together with the data accompanying it, is submitted by the Commander of the E.Y.P. to the President of the Parliament, in order to grant the relevant permission within twenty-four (24) hours. If there is no Parliament, the permission of the second paragraph is granted by the President of the last Parliament or, if he refuses or is not present, the Prime Minister. If the request concerns the President of the Parliament, or if there is no Parliament to the President of the last Parliament, the permission is granted by the Prime Minister. Only if the present permission is granted, the request can be submitted to the prosecutor's office of par. 3 of article 5 of Law 3649/2008 for the continuation of the procedure. In the present case, the President of the Parliament, the President of the last Parliament or the Prime Minister, as the case may be, does not keep a relevant record.

4. The provision requiring the declassification of communications for reasons of national security contains:

a) the body requesting the removal,

b) the purpose of the removal,

c) the means of response or communication in which the removal is imposed,

d) the object of the removal, i.e. the external elements of the communication or its content,

e) the territorial extent of application, if required for the needs of the removal, and the absolutely necessary time duration of the removal and

f) the date of issuance of the provision.

5. An order denying a request to declassify communications for reasons of national security contains only:

a) the institution that had requested the removal, and b) the date of issuance of the order.

6. The provisions that impose the removal of confidentiality or reject the relevant request, are kept in an electronic file of the Service by the competent prosecutor's officer of par. 2. By decision, as the case may be, of the Governor of the E.Y.P. or of the Director of DAEEB, the physical files of the declassification provisions for reasons of national security are digitized and integrated into the electronic file of the first paragraph. In this decision, the method and process of digitization are defined. After the lapse of one (1) year from the digitization, the physical begins a are destroyed and a report is drawn up on their destruction.

7. After the expiry of three (3) years from the termination of the validity of the provision for the removal of confidentiality for reasons of national security, the imposition of the restrictive

measure shall be notified to the affected person, provided that the purpose for which it was ordered is not compromised. For the disclosure of the first paragraph, a relevant request is submitted to the Authority for Ensuring the Privacy of Communications (A.D.A.E.), which is forwarded to the E.Y.P. and D.A.E.E.B.. The removal is notified after a decision of a three-member body, which decides within a period of sixty (60) days. In the case of the removal by the E.Y.P., the body consists of the prosecutor's officer of par. 3 of article 5 of Law 3649/2008, the second prosecutor's officer of par. 2 of article 4 hereof and the President of the A.D.A.E.. In the case of the removal by the A.D.A.E.B., the body is composed of the public prosecutor of par. 3 of article 4 of Law 2265/1994, the second prosecutor's officer of par. 2 of article 4 hereof and the President of the A.D.A.E. The body decides by majority vote, keeping confidential minutes and recording the opinion of the minority, if any. If notification is decided, the affected person is informed of the imposition of the restrictive measure and of its duration. It is not allowed to submit a new request before the lapse of one (1) year from the submission of the previous one.

Article 5

Material handling in lifts for national security purposes

1. After the lapse of ten (10) years from the termination of the validity of the prosecutor's order for the lifting of the confidentiality of communications for reasons of national security, it may, following the recommendation of the competent Service as the case may be and with a decision of the relevant three-member body of par. 7 of article 4, to destroy the files with the documentary material for declassification for reasons of national security.

2. If the prosecuting officer of the first paragraph of par. 2 of article 4 judges that the material recorded in the attachment system constitutes evidence for criminal prosecution, it is extracted to a material carrier and sent, with a new provision, to the competent prosecuting authorities. By the same provision, this material is limited to content that is judged to contribute evidence to the investigation of crimes.

3. After the expiration of six (6) months from the termination of the validity of the prosecutor's order for the removal of the confidentiality of communications for reasons of national security, the material recorded in the attachment system is deleted from the system. In the event that the competent Service deems it necessary to preserve the material: (a) for its association with elements under investigation or (b) due to the assistance of par. 2, the material is exported from the system to a material carrier. Without prejudice to par. 2, and if there is a special reason, following a written proposal of the competent Directorate or Department and approval

of the Governor of the E.Y.P. or of the Director of D.A.E.E.B., as the case may be, material recorded before the completion of six (6) months is deleted from the system.

4. Without prejudice to the second paragraph of par. 3, all the information material extracted for the needs of the Service from the connection system in paper form or imprinted on physical carriers, is destroyed within six (6) months from the termination of validity of the prosecutor's order that ordered the declassification of the communications.

5. The material that is not related to the reason for imposing the measure, is destroyed without delay before the authority that issued the order.

6. Where destruction or erasure is provided herein, a report shall be drawn up by the employee authorized for this purpose.

Article 6

Declassification of communications to investigate crimes

1. Declassification of communications is permissible for the determination of the following felonies:

a) of Chapters One, on insults to the democratic state, Second, on insults to the country's international status, Fourth, on crimes against state and political bodies, Sixth, on crimes against public order, Ninth, on crimes related to currency , other means of payment and insignia, Sixteenth, on crimes against bodily integrity, Eighteenth, on crimes against personal freedom, Nineteenth, on crimes against sexual freedom and crimes of economic exploitation of sexual life, Twenty-Second, on insults to individual privacy and communication, as well as articles 235, on bribery of an official, 236, on bribery of an official, 237, on bribery and bribery of a judicial official, 264 on arson, 265 on arson in forests, 270 on explosion, 272 on the manufacture and possession of explosives and of incendiary substances, 290 on dangerous interventions in road transport, 291 on dangerous interference with the transportation of means of fixed orbit, ships and aircraft, 299 on manslaughter, 374 on aggravated theft, 380 on robbery, 385 on extortion, 386 on fraud and 386A on computer fraud of the Special Part of the Criminal Code (law 4619/ 2019, A' 95),

b) of the First Chapter, on insults against the integrity of the country, as well as articles 46, on posture, 47, on group infidelity, 140, on unsealing, smuggling of documents or other objects and 144, on transmission of military secrets, of the Special Part of the Military Criminal Code (law 2287/1995, A' 20),

c) of Law 4557/2018 (A' 139), on money laundering from criminal activities and financing of terrorism, paragraph c of paragraph 1 of Article 157 of the National Customs Code (Law 2960/2001, A' 265), on smuggling, articles 28 and 31 of Law 4443/2016 (A' 232), on criminal

acts of persons possessing privileged information and on criminal market manipulation, respectively, of Article 15 of Law 2168/1993 (A' 147), on weapons, ammunition, explosives and explosive devices, Articles 20, 22 and 23 of Law 4139/2013 (A' 74), on addictive substances, Article 11 of Law 3917/2011 (A ' 22), on data held by the provider of electronic communications services or public communications network, of par. 5 of article 38 of Law 4624/2019 (A' 137), on access to personal data, of Article 28 of Law 1650/1986 (A' 160), on the protection of the environment, of Law 4858/2021 (A' 220), on the protection of antiquities and cultural heritage in general, of paragraph 3 of Article 66 of Law 2121/ 1993 (A' 25), on the protection of intellectual property and related rights, par. 4 of article 132 of Law 2725/1999 (A' 121), on bribery-bribery for altering the result of a match and Article 30 of Law 4251/2014 (A' 80), on the transfer of third country nationals who do not have the right to enter the country.
As amended by Article 44 LAW 5046/2023 effective 7/29/2023
See the development of the paragraph
2. The lifting of confidentiality is permissible for the verification of the following misdemeanors:
a) of articles 148, on espionage, 187, on criminal organization, 187A, on terrorist acts-terrorist organization, 187B, on criminal support, 323A, on human trafficking, 324, on abduction of minors, 339, on sexual acts with minors or before them, 342, on abuse of minors, 343, on sexual abuse, 346, on revenge pornography, 348, 348A, 348B, 348C, 351A, on offenses against minors and pornography, 370F, on monitoring software and devices, 386 , on fraud and 386A, on computer fraud of the Criminal Code,
b) of articles 28 and 31 of Law 4443/2016, on criminal acts of persons possessing privileged information and on market manipulation, respectively, and of the third paragraph of paragraph 1 of Article 44 of Law 3959/2011 (A' 93), on the protection of free competition.
3. For the removal of the confidentiality of communications in the cases of paras. 1 and 2, the competent judicial council decides, within forty-eight (48) hours, with a specially reasoned decision, following a proposal by the public prosecutor. In extremely urgent circumstances the removal may be ordered by the prosecutor or the investigator. In this case, the prosecutor or the investigator is obliged to introduce the matter, within a period of three (3) days, to the competent judicial council, which at the same time controls the presence of extremely urgent circumstances. Otherwise, the validity of the relevant provision is automatically revoked. If a will is not issued within a reasonable time, which cannot exceed five (5) days in total, the findings are not usable.

4. The will or the provision that imposes the lifting of the secrecy for the verification of crimes, includes:

a) the police authority or the prosecutor or the investigator requesting the removal,

b) the criminal act, c) the serious evidence of guilt against the person against whom the removal is carried out, d) the justification for imposing the removal, in particular the impossibility or particular difficulty of ascertaining the crime in another way,

e) the purpose of the removal,

f) the means of response or communication in which the removal is imposed,

g) the object of the removal, i.e. the external elements of the communication or its content, h) the territorial extent of application, if required for the needs of the removal, and the absolutely necessary duration of the removal,

i) the date of issuance of the provision, and

j) the details of the person or persons against whom the removal is imposed.

5. The will or provision that rejects a request to remove privacy contains:

a) the police authority or the prosecutor or the investigator who requested the removal and b) the date of issuance of the order.

6. The lifting of confidentiality can be imposed under the conditions of par. 3 hereof and against a third person not participating in the crime, as long as the conditions of par. 4 of article 254 of the Code of Criminal Procedure (law 4620/2019, A' 96) are met.

7. In the cases of crimes under the jurisdiction of the military courts, the judicial council of the competent military court imposes, by its decision, the removal of secrecy, following a request: a) of the competent prosecutor of the military court, who supervises or acts as a preliminary investigation or preliminary examination or b) of the investigator acting as a routine investigation.

8. A.D.A.E., after the expiration of the measure of the removal of confidentiality and after submitting a relevant request by the affected party, shall notify him of the imposition of this measure within a period of sixty (60) days, with the agreement of the Prosecutor of the Supreme Court and provided that the purpose for which it was ordered is not compromised.

Article 7

Material management in crime detection lifts

1. The data collected or seized and the material captured in execution of the order for the lifting of confidentiality in the event of crime detection are attached to the case file, if they constitute evidence for the criminal prosecution or the acquittal of the accused at the discretion of the issuing authority layout. By order of the competent prosecutor or investigator as the

case may be, the material captured for the purpose of investigating crimes and which is intended to be attached to a case file, is limited to the content that is judged to contribute evidence to the investigation of the crimes for which the declassification was ordered, or in the acquittal of the accused for them.

2. Any information or knowledge obtained during the removal is used in the context of this criminal trial, provided that it concerns an act for which the removal of confidentiality is permitted. Exceptionally, this element or the acquired knowledge is allowed to be used in another criminal trial to prove the crimes of paragraphs 1 and 2 of article 6, if the judicial council decides specifically on this.

3. In the cases of articles 28 and 31 of Law 4443/2016 (A' 232), on criminal acts of persons possessing privileged information and on criminal manipulation of the market, respectively, the material recorded pursuant to paras. 1 and 2 of article 6 hereof and if the judicial council specifically decides on it following a request from the Capital Market Commission introduced to it at the proposal of the competent prosecutor, it is additionally used during the administrative procedure to establish the violations and impose the fines of article 37 of Law 4443/2016, Articles 93a and 94 of Law 4099/2012 (A' 250), as well as items (a) and (b) of Article 14 and Article 15 of Regulation (EU) 596/2014 of the European Parliament and of the Council of April 16, 2014 on market abuse (Regulation on market abuse and repealing Directive 2003/6/EC of the European Parliament and of the Council) and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (L 173) and are attached to the relevant file during the proceedings before the administrative courts. In the case of the third paragraph of paragraph 1 of article 44 of Law 3959/2011 (A' 93), on free competition, the material recorded pursuant to paragraph 2 of article 6 hereof and if the judicial council decides specifically about this at the request of the Competition Commission which is introduced to it at the proposal of the competent prosecutor, it is additionally used during the administrative procedure to establish the violations and impose the fines of article 25B of Law 3959/2011, and is attached to the relevant case file during the proceedings before the administrative courts.

4. In any case, after the issuance of an irrevocable decision or an irrevocable exculpatory will or if no criminal prosecution was brought upon a preliminary examination, the data collected and the material collected are destroyed without delay before the authority that issued the order and a report on the destruction is drawn up.

Article 8

Deprivation process

1. Excerpt of the provision or decree, including the ordinance, is delivered without delay by electronic encrypted message, which meets the security conditions of the confidentiality of the content:

a) To the president or the board of directors or the general manager or the representative of the legal entity to which the means of response or communication belongs. In the case of a sole proprietorship, the above excerpt is delivered to the entrepreneur.

b) In the case of public services or legal entities subject to the control or supervision of the state, the above excerpt is also delivered to the Minister in charge of the public service or to the Minister supervising the legal entity.

2. The entire text of the provisions and decrees that impose the lifting of confidentiality or reject a relevant request shall be delivered without delay in a non-editable form, with an electronic encrypted message that covers the security conditions of the confidentiality of the content, to the A.D.A.E. The provisions and resolutions sent in the above manner to the A.D.A.E. stored and maintained in special electronic files, located in a database system. The storage is carried out by A.D.A.E. staff. specially authorized for this purpose by this Plenary. Access to the special file in question, as well as searching for data, is only carried out by the President of A.D.A.E. and two (2) more members of the Plenary appointed by it. The results of the search are presented at the next meeting of the Plenary. It is forbidden to extract information in any way from the database, and the violation of this prohibition is punishable by imprisonment of at least one (1) year, if the act is not punished more severely by another criminal provision.

3. In the E.Y.P. and in D.A.E.E.B. electronic platforms for the delivery of the provision on the declassification of communications for reasons of national security are created, for the purpose of sending and delivering excerpts of the provisions by electronic encrypted message to the recipients defined in par. 1 and sending and delivering the entire text of the provisions to A.D.A.E..

4. The duration of the removal of confidentiality cannot exceed two (2) months. Extensions, which do not exceed two (2) months each time, can be ordered by the procedure, provided for each case, for the enforcement of the measure and on the condition that the reasons for the removal still exist. In any case, the duration cannot exceed a total of ten (10) months. Exceeding the limit of the second paragraph is only allowed in cases of revocation for reasons of national security, as long as it is based on specific elements that make national security immediately and extremely likely to be endangered, and the continuation of the assistance of these elements is confirmed in every extension of the validity of the revocation. After the

expiration of the removal period or after the expiration of the maximum allowed time limit, the removal of privacy automatically ceases. In any case, by order of the body that imposed the removal, it is ordered to cease even before the expiration of its certain duration, if the purpose has been fulfilled or the reasons for imposing the measure have disappeared.

5. After the execution of the provision or decree, one or more reports are drawn up, depending on the circumstances, by the agency that carried out the acts of declassification. The reports are signed by an authorized employee of the service of the first paragraph and they state:

a) the actions taken to execute the order,

b) the place, date and method of execution of the above actions,

c) the name of the employees who carried them out.

Copies of these reports are forwarded with proof, in a closed file, to the requesting authority, to the judicial authority that issued the order or will and to the A.D.A.E.

6. The President of A.D.A.E. informs the President of the Parliament, the leaders of the parties represented in the Parliament and the Minister of Justice about issues of declassification of communications.

7. Without prejudice to paragraphs 2 and 3 of article 5 and paragraphs 2 and 3 of article 7, the content of the response or communication, which became known due to the lifting of confidentiality, as well as any other related information it is prohibited, under penalty of invalidity, to be taken into account as direct or indirect evidence in another criminal, civil and administrative trial and administrative procedure for a purpose other than that which was determined by the provision.

8. The competent employee of the legal entity that owns the means of response or communication for which the removal was imposed shall be punished with imprisonment of at least six (6) months, if he does not provide the requesting authority with information related to the content of the provision and technical or official information in general assistance for its execution. An employee of the law is punished with imprisonment of at least two (2) years of the person who owns the means of response or communication for which the removal was imposed, if he discloses the fact of the removal of privacy, or communicates to third parties or uses the content of any kind of messages, information and data that came to his knowledge due to the removal of confidentiality or violates his obligation of confidentiality during the procedure of lifting the confidentiality provided for by article 8 of the p.d. 47/2005 (A' 64).

9. By decision of the Plenary Assembly of ADAE, the provisions and decrees on the lifting of confidentiality, which have been stored in physical files at the Authority since its establishment, are digitized and stored in the special electronic files of par. 2 Digitization and

storage is carried out by the Authority's staff specially authorized by the Plenary. After one (1) year has passed since their digitization, the physical records are destroyed and a report is drawn up on their destruction.

Article 9

Judicial officers of the E.Y.P. and of D.A.E.E.B. Amendment of paragraph 3 of article 5 of law 3649/2008 and paragraph 3 of article 4 of law 2265/1994

1. The first paragraph of par. 3 of article 5 of Law 3649/2008 (A' 39) is amended in terms of the term of office of the public prosecutor's office. and par. 3 is formulated as follows:

"3. In E.Y.P. a public prosecutor is appointed, following a decision of the Supreme Judicial Council, for a non-renewable three-year term, who checks the legality of its special operational actions concerning human rights issues and exercises any other powers assigned to him by the provisions of this law. If the public prosecutor is absent or for any reason obstructed, he is replaced by the public prosecutor provided by the provision of article 4, paragraph 3 of Law 2265/1994."

2. The first paragraph of paragraph 3 of article 4 of Law 2265/1994 (A' 209) is amended with regard to the term of office of the public prosecutor provided for in this provision, who supervises the D.A.E.E.B. , in accordance with paragraph 6 of article 22 of Law 4249/2014 (A' 73), and paragraph 3 of Article 4 of Law 2265/1994 is formulated as follows:

"3. The aforementioned Council is established by a decision of the Minister of Citizen Protection and consists of a public prosecutor, as chairman, who is appointed by decision of the Supreme Judicial Council with full and exclusive employment, for a three-year term that cannot be renewed, and of six (6) senior or senior officers of the Greek Police, as members. If the public prosecutor is absent or is obstructed for any reason, he is replaced by the public prosecutor provided by the provision of article 5 par. 3 of Law 3649/2008. In the case of examination, study or analysis of special matters within the competence of the Council, scientists specialized in these matters may also participate, who are hired under a project lease contract or serve in the Ministry of Citizen Protection in any employment relationship. By decision of the Ministers of Citizen Protection and National Defense, it is possible for officers of the Armed Forces to participate in the Council. In the event that the prosecuting authorities conduct, in accordance with the provisions of the Criminal Procedure Code, a preliminary investigation or a preliminary examination for cases of special crimes of violence, the public prosecutor who participates in the council, in addition to the duties he exercises under the provisions of par. 5 of the same article issued presidential decree, he himself acts at his discretion the above preliminary investigation or preliminary examination."

CHAPTER III MONITORING SOFTWARE

Article 10

Violation of confidentiality of telephone communication and oral conversation Amendment of Article 370A of the Civil Code

In article 370A of the Criminal Code (law 4619/2019, A' 95) the first paragraph of pars. 1 and 2 and par. 4 are amended in terms of the penalty framework, in par. 3 the word "unlawful" is deleted and amended the penalty framework, par. 5 is added and article 370A is formulated as follows:

"Article 370A Violation of privacy of telephone communication and oral conversation

1. Anyone who unlawfully traps or in any other way interferes with a device, connection or network for the provision of fixed or mobile telephony services, or with a hardware or software system, used for the provision of such services, with the aim of obtaining information or recording in carrier material, the content of a telephone conversation between third parties or communication data (motion and location) is punishable by imprisonment of up to ten (10) years. The act of the previous subsection is punished with the same penalty when the perpetrator captures on a physical medium the content of his telephone communication with another, without the express consent of the latter.

2. Anyone who unlawfully monitors with special technical means or captures on a physical medium an oral conversation between third parties that is not conducted in public or captures on a physical medium a non-public act of another, shall be punished with imprisonment of up to ten (10) years. The act of the previous paragraph is punished with the same penalty when the perpetrator captures on a physical medium the content of his conversation with another without the express consent of the latter.

3. Whoever makes use of the information or the material carrier on which it has been recorded in the ways provided for in paragraphs 1 and 2, shall be punished by imprisonment of up to ten (10) years.

4. If the perpetrator of the acts of paragraphs 1, 2 and 3 is a telephone service provider or its legal representative or a member of the administration or a person responsible for safeguarding privacy or an employee or partner of the provider or conducts private investigations or performs these acts professionally or aimed at the collection of remuneration, imprisonment of up to ten (10) years and a fine is imposed.

5. If the acts of paragraphs 1 and 3 constitute a violation of military or diplomatic secrecy or concern secrecy referring to the security of the state or the security of public utility facilities, imprisonment shall be imposed."

Article 11

Violation of non-public transmissions of data or electromagnetic emissions Amendment of Article 370E PC

In article 370E of the Criminal Code (law 4619/2019, A' 95), paragraph 1 is amended in terms of the penalty framework, paragraph 3 is added and article 370E is formulated as follows:

"Article 370E 1. Whoever, unlawfully, by the use of technical means, monitors or captures on a material carrier non-public data transmissions or electromagnetic emissions from, to or within an information system or interferes with them with the aim of himself or another being informed of their content , is punishable by imprisonment of up to ten (10) years.

2. Whoever makes use of the information or the material carrier on which it has been recorded in the ways provided for in paragraph 1 shall be punished with the penalty of paragraph 1.

3. If the acts of paragraphs 1 and 2 constitute a violation of military or diplomatic secrecy or concern secrecy relating to the security of the State in time of war, imprisonment shall be imposed."

Article 12

Prohibition of circulation of software, monitoring devices and other data Addition of Article 370F of the Civil Code

A new article 370F is added to the Criminal Code (law 4619/2019, A' 95) as follows:

"Article 370F Prohibition of traffic of software, monitoring devices and other data

1. Anyone who produces, sells, procures for use, imports, exports, owns, distributes or otherwise traffics in software or monitoring devices with the possibility of interception, recording and any kind of extraction of content or data shall be punished with imprisonment of at least two (2) years communication (movement and location), with which the acts of article 370A can be carried out.

2. Whoever, without the right and with the intention of committing any of the crimes of articles 370B, 370C, paragraphs 2 and 3 of article 370D and article 370E, produces, sells, supplies for use shall be punished with imprisonment of at least two (2) years , imports, exports, possesses, distributes or otherwise traffics passwords or access codes or other similar data, with the use of which it is possible to gain access to all or part of an information system."

Article 13

Procurement of monitoring software and devices by the State

By presidential decree, issued within three (3) months from the entry into force of this, following a proposal by the Ministers of Citizen Protection, National Defence, Justice and Digital Governance, the conditions under which it is permissible to enter into contracts on

behalf of state structures for the supply of software or monitoring devices of article 370F of the Criminal Code for the fulfillment of their purposes, as well as additional terms of their use.

Article 14

Update for tracking software or devices

Monitoring software or devices are recorded in an indicative list issued by the Plenary of A.D.A.E. following a recommendation from the Coordination Committee for Cybersecurity issues of article 20. The list of the first paragraph is updated every six (6) months at the latest. By the E.Y.P.'s Governor, informative material on the software of the first paragraph, their mode of action and the protection measures that can be taken against them is posted on the website of the Service.

CHAPTER D: E.Y.P. Issues

Article 15

Structure of E.Y.P. Amendment of paragraph 4 of article 3 of Law 3649/2008

Paragraphs d and e are added to paragraph 4 of article 3 of Law 3649/2008 (A' 39) and paragraph 4 is formulated as follows:

"4. In E.Y.P. works: a. Office of Legal Counsel of the State Legal Council. b. Service of Historical Archive and Historical Museum, which reports directly to the Governor of the E.Y.P., whose main task is the classification and utilization of documents and audio-visual material, as well as the classification and preservation of materials of museum value. These documents and material are declassified after 50 years have passed, by decision of the Commander of the E.Y.P., following the opinion of a Three-member Declassification Committee, made up of employees of the E.Y.P., by decision of the same. Excluded from declassification are documents and materials that are in the computerization stage, those that have worn out and require maintenance, as well as those whose disclosure could harm national interests or rights deriving from personality.

c. An autonomous service, called the Center for Technological Support, Development and Innovation (K.T.Y.A.K.), which operates at the Directorate level and reports directly to the Commander of the E.Y.P.. The service of the first paragraph is responsible for conducting applied research, collaborating with Greek and foreign research bodies, coordinating, as well as monitoring and participating in research, technological development and innovation activities, in order to create the appropriate technological and methodological tools and provide them to E.Y.P. and to other public bodies.

d. E.Y.P. Internal Control Unit, which operates at the level of a Sub-Directorate within the Security Directorate, applied in accordance with article 39 of Law 4622/2019 (A' 133). Its structure and responsibilities are provided for in the Organization of the Service and the internal regulation issued in accordance with articles 11 and 12 hereof.

e. Press and Communication Office, which reports directly to the Commander of the E.Y.P.. The Press and Communication Office is responsible, in particular, for promoting the work of the E.Y.P. and to inform society about the actions of the Service and about risks to national security."

Article 16

Operation of the Center for Technological Support, Development and Innovation (KE.TY.A.K.) and strengthening of transparency Amendment of paragraph 2 of article 3A of law 3649/2008 and paragraph 5 of article 38 of law 4412/2016

1. In paragraph 2 of article 3A of Law 3649/2008 (A' 39), paragraph b of the first paragraph is amended as regards the conditions of employment of the staff of E.Y.P. and the second paragraph, so that the non-publication in the Government Gazette and the non-posting in the Clarity program are referred to exclusively in para. b of the same paragraph and para. 2 is formulated as follows:

"2. In the context of undertaking and executing a project, which is either financed in its entirety or co-financed at a rate of at least fifty percent (50%) from European or private resources, the KE.TY.A.K. may, by decision of its Governor E.Y.P.: a) to enter into project contracts with natural persons, researchers and specialized scientific personnel, b) to employ all kinds of personnel from the employees with any employment relationship at E.Y.P. and beyond their working hours. The acts of paragraph b' are not published in the Government Gazette and are not posted in the Clarity program."

2. A new third paragraph is added to paragraph 5 of article 38 of Law 4412/2016 (A' 147) and paragraph 5 is formulated as follows:

"5. For reasons of national security, the elements of par. 3 and 4, as well as any other element defined by the decision of par. 6, concerning the Armed Forces, are registered in a classified information system, subject to compliance with the security regulations of Ministry of National Defense. For reasons of national security, the elements of pars. 3 and 4, as well as any other element defined by the ministerial decision of par. 6, concerning the National Intelligence Service (NIS), are excluded from registration in the KIMDIS. The second paragraph does not apply to public contracts for which the contracting authority is the Center for Technological Support, Development and Innovation, established by Article 3 of Law

3649/2008 (A' 39), which do not fall within the scope of the Special of the Public Contracts Regulation of par. 2 of article 20 of Law 3649/2008 and for which the data of para. (b) of par. 3 hereof are registered in KIMDIS as follows: Contract title, CPV codes, Contract budget, Project /Sub-project financing the contract, Brief description of physical object of contract. For reasons of national security, the elements of par. 3 and 4, as well as any other element defined by the ministerial decision of par. 6, relating to contracts concluded by the Services of the Ministry of Foreign Affairs and characterized as confidential or the conclusion and their execution, must be accompanied by special security measures, registered in a classified information system, subject to compliance with the security regulations of the Ministry of Foreign Affairs. With a joint decision of the relevant Minister and the Minister of Digital Governance, the manner of submitting the data, access to it, as well as any other matter related to the implementation of this regulation shall be regulated.

Article 17

Information Security Authority Issues (INFOSEC) Amendment of section 7 of article 4 of Law 3649/2008

In para. 7 of article 4 of Law 3649/2008 (A' 39), the first paragraph is updated regarding the competences of the E.Y.P. and the referenced legislation, two new paragraphs are added at the end of the case and para. 7 is formulated as follows:

"7. It is a Technical Information Security Authority (INFOSEC), National "CRYPTO" Authority, National "TEMPEST" Authority and ensures, in accordance with the provisions of paragraph 5 of article 2 of the p.d. 1/2017 (A' 2), for the security of national communications and information technology systems, as well as for the certification of classified national communications material. The certification is provided against the payment of an electronic fee, the amount of which is determined by a joint decision of the Prime Minister and the Minister of Finance. In addition, as the Information Security Authority (INFOSEC) it is responsible for establishing instructions regarding the drafting of security policies and the management of classified information in all networks and areas of the Presidency of the Government and the Ministries, in cooperation with them, as well as for the constantly updating them on safety issues. The previous paragraph does not apply to the Ministry of National Defense and its affiliated bodies."

Article 18

Administration of E.Y.P. Amendment of par. 2 and replacement of par. 4 of article 9 of Law 3649/2008

1. A new first paragraph is added to paragraph 2 of article 9 of Law 3649/2008 (A' 39) and paragraph 2 is formulated as follows:

"2. An ambassador or plenipotentiary minister A' or an ambassador ex officio or plenipotentiary minister A' ex officio or a retired officer of the armed forces or the security forces who held the rank of a senior officer in action is appointed commander. The Commander is a transferable employee of the category of special positions with grade 1. Appointed and dismissed freely by decision of the competent member of the Government. The appointment is carried out after the opinion of the competent committee of the Parliament, in accordance with the provisions of its Rules of Procedure."

2. Paragraph 4 of Article 9 of Law 3649/2008 is replaced as follows:

"4. The Commander is assisted in his work by two Deputy Commanders. Deputy Commanders carry one of the qualities provided for the position of Commander. Duties of Deputy Governors may also be assigned to active or retired public sector employees and functionaries within the meaning of paragraph (a) of paragraph 1 of article 14 of Law 4270/2014 (A' 143). The Deputy Commanders are transferable employees of the category of special positions with grade 2 and are appointed and dismissed freely by decision of the competent member of the Government."

Article 19

Academy of Information and Counterintelligence E.Y.P. Amendment of paragraph 1 of article 13 of Law 3649/2008

Paragraph 1 of article 13 of Law 3649/2008 (A' 39) is replaced as follows:

"1. An Academy of Information and Counterintelligence E.Y.P. is established, which operates at the Directorate level, the structure and affiliation of which are provided for in the Organization of the E.Y.P. and the internal regulations issued in accordance with articles 11 and 12. The mission of the Academy is the education, training and specialization of the staff of the E.Y.P. for the more efficient execution of his duties. By decision of the competent member of the Government, following a proposal by the Governor of the E.Y.P., the Academy's Operating Regulations are approved. The Regulations regulate the matters of establishment, operation and organization of the Academy, the duration of the trainings, the way of preparing teaching programs and any other relevant matter. For all matters not regulated in the Academy's Operating Regulations, the internal regulations and the attached table of composition and distribution of the staff of the E.Y.P. are applied. The Academy's Operating Regulations are confidential and are not published in the Government Gazette."

CHAPTER E CYBERSECURITY ISSUES

Article 20

Establishment of a Coordination Committee for Cyber Security issues

1. A Coordinating Committee for Cyber Security issues is established.

2. The Committee is the coordinating body between: a) the General Directorate of Cybersecurity of the General Secretariat of Telecommunications and Posts of the Ministry of Digital Governance, which has been designated as the National Cybersecurity Authority according to Law 4577/2018 (A' 199),

b) of the Directorate of Cyber Defense of the General Staff of National Defense, designated as the competent response team for computer security incidents (Computer Security Incident Response TeamCSIRT),

c) of the Directorate of Cyberspace of the E.Y.P. as a cyber attack response team (National CERT) and

d) of the Greek Police.

Article 21

Committee Mission

The Cyber Security Coordinating Committee is tasked with planning, monitoring, coordinating actions, intervening in issues related to cyber security from the initial stage of prevention to the stage of effective response to cyber-attack incidents and minimizing the impact of cyber threats.

Article 22

Committee Responsibilities

The responsibilities of the Coordinating Committee for Cyber Security issues are as follows:

a) provides directions in the event of an extraordinary event involving a strategic risk and may designate one of the entities of par. 2 of article 20 as the primary operational entity, in derogation of any general or special provision that defines the responsibilities of each entity. The primary operational entity coordinates the actions of other entities with the aim of achieving the optimal level of information security, personal data and information systems in the country, as well as monitoring and preventing risks and incidents in the context of cyber attacks,

b) coordinates, monitors and evaluates the implementation of the National Cybersecurity Strategy, by the bodies of par. 2 of article 20, according to the reason of competence of each one, to ensure its uniform and effective implementation for the benefit of the public interest,

c) approve the National Emergency Plan, which is the guide for dealing with events that are judged to be serious disruptions to the services provided by the agencies involved, which includes, in particular, the procedure manual, and the criteria, which categorize a event as an extraordinary event involving strategic risk,

d) recommends to the Governmental National Security Council any issue related to Cybersecurity,

e) remove any disagreements regarding the competences of the bodies of par. 2 of article 20 in matters of Cybersecurity,

f) recommends to the Plenary Assembly of A.D.A.E. the list of monitoring software or devices in article 14.

Article 23

Formation and functioning of the Committee

1. The Cybersecurity Coordination Committee consists of six (6) members as follows:

a) the five (5) members are employees or functionaries of the public sector, as defined in para. a of par. 1 of article 14 of Law 4270/2014 (A' 143) and are indicated one by one by the Minister of National of Defense, the Minister of Citizen Protection, the Minister of Digital Governance, the responsible for the supervision of the E.Y.P. member of the Government or the person responsible for the supervision of the E.Y.P. Deputy Minister and the Commander of the E.Y.P.,

b) the sixth member is the head of the Office of the National Security Adviser of the General Secretariat of the Prime Minister of article 23 of Law 4622/2019 (A' 133), who chairs the Committee.

The members of the Committee are appointed by decision of the person responsible for the supervision of the E.Y.P. member of the Government. The term of office of the members of the Committee is four years and may be renewed only once (1). Committee members are freely recalled by the bodies that appoint them.

2. The Committee may continue to operate if any of its members disappear or withdraw for any reason, as long as the other members are sufficient to form a quorum.

3. The Committee meets regularly at least every one (1) month, upon the invitation of the President and exceptionally, upon the invitation of the President or at the request of at least three (3) of its members. Members are invited by the President in any convenient way and the invitation includes the items on the agenda. The Committee may also meet via teleconference, if this is deemed feasible by the President, taking into account the critical and confidential nature of the issues on the agenda.

4. The decisions of the Committee are taken by a majority of the members present. In case of a tie, the vote of the President prevails.

5. The Committee may participate, without the right to vote, if invited by it, public officials and employees, all kinds of executives employed by the public sector, private experts, as well as members of the working groups of article 24.

6. The members of the Committee, as well as the persons summoned pursuant to par. 5, have a classification corresponding to the incident, with the highest being Top Secret.

Article 24

Commission working groups

1. To assist in its responsibilities, the Coordination Committee for Cybersecurity issues may recommend working groups, consisting of specialized public sector personnel and private experts, define their organization and functioning and monitor their work.

2. Within the scope of their responsibilities, the working groups may consult with officials of the public sector, Basic Services Operators of section 4 of article 3 and Digital Service Providers of section 6 of article 3 of Law 4577/2018 (A' 199), as well as private bodies for the exchange of views and ensuring the collaborations required for the effective prevention and management of crises in cyberspace.

Article 25

Committee administrative support

The administrative support of the Committee is entrusted to the Presidency of the Government. The Committee's needs are covered by appropriations from the Presidency of the Government.

Article 26

Obligation to inform and provide assistance

1. All public sector bodies, within the meaning of paragraph a of paragraph 1 of article 14 of Law 4270/2014 (A' 143), in particular the prosecution authorities, the Personal Data Protection Authority, the .D.A.E. and the National Commission for Telecommunications and Posts, are obliged to inform without delay the bodies of par. 2 of article 20 as soon as they receive any information about a cyber-attack that is in progress or has been completed.

2. The primary operational entity of paragraph (a) of article 22 may request from the public services and other entities of the public and private sector, as well as from individuals, any information or document or any element, which they transmit within twenty-four (24) hours.

3. Any information or document referred to in paragraph 2 is classified in any case as confidential or, exceptionally, as highly confidential.

4. For the transmission of information or documents, the confidentiality of the information is ensured by all the necessary technical means, in accordance with the provisions of the Interbranch Military Correspondence Regulation.

Article 27

Support for actions of the national coordination center of par. 1 of article 17 of Law 4961/2022 Amendment of par. 2 of article 17 of Law 4961/2022

Paragraph 2 of article 17 of Law 4961/2022 (A' 146) is amended in terms of the competent body for planning and supporting the implementation of the actions of the national coordination center of paragraph 1 of the same article and is formulated as follows:

"2. The public limited company of the Greek State "Information Society Sole Proprietorship S.A." (K.t.P. M.A.E.) is responsible for the management, planning and support of the implementation of special actions, which have received grants from the European Center of Competence for Industrial, Technological and Research Cybersecurity Issues, between others, through financial support from third parties, in accordance with article 204 of Regulation 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) 1296/2013 , (EU) 1301/2013, (EU) 1303/2013, (EU) 1304/2013, (EU) 1309/2013, (EU) 1316/2013, (EU) 223/2014, (EU) 283/2014 and of Decision 541/2014/EU and for the repeal of Regulation (EU, Euratom) 966/2012 (L 193), under the conditions provided for in the corresponding grant agreements."

Article 28

Monitoring IT and communications system threats and vulnerabilities

1. The National Cyber Security Authority (NAC) and the Directorate of Cyberspace of the E.Y.P. take care, according to their competence, to monitor threats and vulnerabilities of IT and communications systems and to provide information about them.

2. In the context of the above care: a) the E.A.K. issues security notices and recommendations, which it addresses to the Operators of Basic Services of paragraph 4 of article 3 and the Digital Service Providers of paragraph 6 of article 3 of Law 4577/2018 (A' 199) and b) the Cyberspace Directorate of E.Y.P. issues security notices and recommendations, which it addresses to the agencies of the Central Government within the meaning of paragraph c of paragraph 1 of article 14 of Law 4270/2014 (A' 143).

3. The security notices and recommendations of par. 2 are communicated by any appropriate means to the relevant bodies, who are obliged to comply with them without delay.

Article 29

National Risk Assessment Plan for Information and Communication Technology systems

The National Cyber Security Authority, in collaboration with the Directorate of Cyberspace of the National Security Agency, the Directorate of Cyber Defense of the Hellenic Police and any other competent body, is preparing a National Risk Assessment Plan for Information Technology and Communications (ICT) systems, which classified according to the National Security Regulation. The draft of the first paragraph includes the identification, analysis and assessment of risks and their impact on the security of ICT systems at the national level. For the preparation of the plan, every category of potential threat is taken into account, and in particular threats related to malicious actions, natural phenomena, technical failures, malfunctions or human errors, in order to assess the extent and criticality of the impact of these threats at the national level.

Article 30

Staffing of the National Cyber Security Authority Amendment of paragraph 5 of article 50 of Law 4635/2019

In par. 5 of article 50 of Law 4635/2019 (A' 167) the following changes are made: a) the first paragraph is amended in terms of the personnel that may staff the National Cybersecurity Authority, b) a new fourth paragraph is added, c) in the old sixth paragraph the categories of civil servants are specified and paragraph 5 is formulated as follows:

"5. The staff positions of the General Directorate of Cyber Security may be filled by: a) all kinds of employees of the Ministry of Digital Governance, b) all kinds of civil servants or officials who serve in other public sector bodies, as defined in paragraph a' of par. 1 of article 14 of Law 4270/2014 (A' 143) through secondment and c) lawyers with a salaried mandate from the State who serve in the bodies of paragraph b', through secondment. In the event that staff positions are covered by secondments from the above agencies and services, the provisions of article 55 of Law 4623/2019 (A' 134) apply. In the event that the agency of origin of the employees is the National Intelligence Service, the Ministry of National Defense, the Ministry of Citizen Protection and the Coast Guard of the Ministry of Shipping and Insular Policy, their secondment requires the consent of the agency of origin. In the event that the source body of the employees is a first or second grade local government organization, the consent of the relevant mayor or regional governor is required, respectively. Secondments are carried out in vacant positions as long as they exist, and also based on the service needs in personnel positions, for which the secondees must possess the required formal qualifications. The recommended personal positions are abolished by the departure of the secondees who hold them in any way. The time of secondment is counted for any consequence as the time of

actual service of the public official or employee, civil or military, in the position he or she holds organically. Secondees, at the time of their secondment, are paid and insured by the organization of their origin, and continue to receive the additional salaries, allowances and insurance coverage that they may have received from it before the secondment, with the sole exception of the position of responsibility allowance."

Article 31

Unified Cybersecurity Reporting Center (Security Operations Center SOC) National SOC Network

1. a) In the General Directorate of Cyber Security of the General Secretariat of Telecommunications and Posts of the Ministry of Digital Governance is recommended and operates a Unified Cybersecurity Reference Center. The purpose of the Unified Cyber Security Reference Center (hereinafter Unified SOC) is to develop, support and strengthen the capabilities at the national level for the early detection and response to cyber threats throughout the Territory, in particular by strengthening the capabilities of early warning, detection and response to cyber attacks. To achieve its purpose, the Unified SOC is defined as the central point of the National SOC Network, which consists of the sector SOCs and supports the organizations participating in it in the identification, management, response and recovery from cyber-attacks.

b) The Unified SOC processes information and data, which are transmitted to it by the organizations and infrastructures that make up the National SOC Network, as well as from every available source. The Unified SOC in particular: b) performs real-time monitoring and analysis of data from public network traffic, with the aim of detecting malicious behavior and incidents affecting the resilience of network and information systems, b) creates a common pool of knowledge, which is shared with the SOC National Network, providing support, guidance and good practices, c) use cutting-edge tools, platforms, infrastructure and technologies for the secure processing and exchange of data and "big data" within the SOC National Network, including artificial intelligence and machine learning technologies; bd) supports and ensures the increased availability, quality, usability and interoperability of information data within the National SOC Network and develops a common situational awareness, b) provides data, support and information in particular to the SOCs that make up the National SOC Network, to the existing CERTs /CSIRTs, in Information Analysis and Sharing Centers (ISACs), in critical infrastructures of the country of the public or private sector and, as the case may be, collaborates with cyber security organizations and businesses inside and outside the country, bst) may, as a single central hub and single central point of

reference of the existing SOCs at the national level, to exchange data with corresponding SOCs of other European Union (EU) member states in the framework of the implementation of the European Cybersecurity Strategy and joint action to strengthen cyber security capabilities at the EU level. Uh..

2. a) The SOC National Network must include: aa) all bodies that fall under point c of paragraph 1 of article 14 of Law 4270/2014 (A' 143) and the government clouds of Article 87 of Law . Article 21 of Law 4961/2022 (A' 146). The above bodies join the National SOC Network either by priority, through a sectoral SOC, if it exists, or directly. SOC National Network operators send automated real-time data to the Unified SOC. The Unified SOC may also accept in an automated or non-automated manner, in real time or asynchronously, data from other sources as well.

b) The Unified SOC, within the framework of the operation of the National SOC Network: b) is the central point of contact, b) operates a "cyber hotline" to support the National SOC Network, b) has specialized staff to detect and deal with cyber threats and of incidents, bd) operates an early warning system and provides instructions in near real time to the organizations of the Network, b) prepares manuals of procedures and incident management rules.

3. To support the Unified SOC and the National SOC Network, the General Directorate of Cyber Security operates an Analyses, Tests and Studies Laboratory to carry out vulnerability analyses, as well as analyzes in particular of malicious codes and software. The purpose of the Laboratory is to promote and exploit applied scientific research in cyberthreats, the study and analysis of malicious software, as well as in the general safe operation of Information Technology and Communications (ICT) systems.

4. In the event that personal data is processed within the framework of the operation of the Unified SOC and the National SOC Network, the provisions of the Union and national legislation on the protection of personal data shall be applied. In any case, before the start of processing operations, an impact assessment is carried out regarding data protection and all appropriate protection measures are applied, while the exercise of all data subjects' rights is ensured, among others, by issuing and implementing a special personal data protection policy.

Article 32

Authorizing provisions for cybersecurity issues Addition of Article 14A to Law 4577/2018

In Law 4577/2018 (A' 199), a new article 14A is added as follows:

"Article 14A Authorizing provisions

1. By decision of the Minister of Digital Governance, issued following the recommendation of the National Cyber Security Authority, every more specific matter is determined regarding:
a. The methodology, the conditions and the specification of the criteria for the determination of the F.E.V.Y., in accordance with par. 2 of article 4 and the characterization of a
event as a serious disturbance according to par. 2 of article 5.
b. The security requirements and the event notification procedure by F.E.V.Y. and P.P.S.Y., in accordance with articles 9 and 11, respectively, for the prevention and minimization of the effects of incidents, and the management of risks related to the security of the network and information systems they use in their activities, and Especially:
wow the determination of the methodology for assessing the suitability of the technical and organizational measures taken by FEVY. and P.P.Y. and
BB. in particular issues related to the process of notifying incidents to the competent authorities as the case may be.
c. The conformity assessment of FEVY. and P.P.Y. regarding the application of articles 9 and 11, respectively, as well as the procedure for providing information, in accordance with paragraph b of paragraph 1 of article 10 and paragraph b of paragraph 1 of article 12, respectively and
d. the instruments, the procedure, the methodology and the standards of inspections and controls of FEVY. and P.P.Y. by the National Cybersecurity Authority.
2. A similar decision may determine any matter related to the measures and the procedure for imposing the sanctions of article 15, including the possibility of their adjustment."

Article 33

Extension of the scope to other entities Addition of Article 14B to Law 4577/2018
In Law 4577/2018 (A' 199), a new article 14B is added as follows:
"Article 14B Extension of scope to other entities
1. Without prejudice to more specific provisions for the security of Information Technology and Communications of entities that do not fall within the scope of the present, paragraphs 1, 2 and 5 of article 9, as well as article 10 may be applied accordingly to these entities in accordance with the specifics defined in the decision of par. 2 hereof.
2. By decision of the Minister of Digital Governance, following the recommendation of the National Cyber Security Authority, other bodies of the public or private sector may be included in the scope of this application and any more specific issue related to:
a. the sectors, sub-sectors, the type of entities or services that may be subject to the provisions herein,

b. the methodology, the conditions and the specification of the criteria for the inclusion of entities in the provisions hereof,

c. the security requirements they must comply with,

d. the conditions, the competent authorities and the procedure for notifying them of an incident, and

e. the conformity assessment, as well as the instruments, procedure, methodology and standards for carrying out inspections and audits."

CHAPTER F SECURITY OF PERSONAL DATA

Article 34

Definition of the data protection officer in public bodies Replacement of par. 5 of article 6 of Law 4624/2019

Paragraph 5 of Article 6 of Law 4624/2019 (A' 137) is replaced as follows:

"5. The public body publishes the contact information of the Ministry of Foreign Affairs. It also informs the Authority of the name and contact details of the FSA."

Article 35

Scope of Law 4624/2019 Replacement of Article 43 Law 4624/2019

Article 43 of Law 4624/2019 (A' 137) is replaced as follows:

"Article 43 Object Scope (articles 1, 2 and 9 par. 2 of the Directive)

1. The provisions of this Chapter regulate the protection of natural persons against the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including protection against threats against of public safety and their prevention.

2. This Chapter applies to the processing of personal data by the competent authorities for the purposes specified in paragraph 1.

3. The processing carried out by the competent authorities for purposes other than those provided for in par. 1, is subject to the provisions of the GDPR, where it is applied, and Chapters A', B' and C' hereof."

Article 36

Definitions Amendment of articles 44, 53, 58 and 71 of Law 4624/2019

1. The number 1 before the only paragraph of article 44 of Law 4624/2019 (A' 137) is deleted.

2. Paragraph n) of article 44 of Law 4624/2019 is replaced as follows:

"n) "competent authority": (n) any public authority responsible for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the protection against and prevention of threats to public security; or
iv) any other public or private organization or entity entrusted with the role of public authority and the exercise of public powers for the purposes of preventing, detecting or prosecuting criminal offenses or enforcing criminal sanctions, including protection against threats to public order security and their prevention."
3. Subsection (e) of Article 44 of Law 4624/2019 is replaced as follows:
"o) "supervisory authority": the Personal Data Protection Authority (hereinafter: Authority), or, for the other Member States, the independent administrative authority established by them, in accordance with Article 41 of Directive (EU) 2016/680."
4. Paragraph q) of article 44 of Law 4624/2019, on the definition of "consent" is repealed.
5. a) In paragraph g) of article 44 of Law 4624/2019, on the definition of the "controller", the word "public" is replaced by the word "competent" and paragraph g) is formulated as follows:
"g) "controller": the competent authority which, alone or jointly with others, determines the purposes and manner of processing personal data."
b) In paragraph i) of article 44 of Law 4624/2019, on the definition of the "recipient", the words "public" and "public" are replaced, respectively, with the words "competent" and "competent" and the i) is formulated as follows:
"i) "recipient": the natural or legal person, competent authority, agency or other entity, to whom the personal data is disclosed, whether it is a third party or not. However, competent authorities that may receive personal data in the context of a specific investigation, in accordance with Union or other law, are not considered recipients. The processing of this data by said competent authorities is carried out in accordance with the applicable data protection rules depending on the purposes of the processing.
c) In the introductory paragraph of Article 53 of Law 4624/2019, on general information regarding data processing, the word "public" is replaced by the word "competent" and Article 53 is formulated as follows:
"Article 53 General information on data processing (Articles 12 and 13 of the Directive)
The data controller provides general and easily accessible information to the public in simple and comprehensible language and through the website of the competent authority regarding:
a) the purposes of the processing, b) the right of the subject to ask the
controller access, correction, deletion or restriction of processing,
c) the identity and contact details of the data controller and the DPO,

d) the right to submit a complaint to the Authority, and
e) the contact details of the Authority."
d) In the first paragraph of paragraph 1 of article 58 of Law 4624/2019, on the right to submit a complaint to the Authority, the word "public" is replaced by the word "competent" and paragraph 1 is formulated as follows:
"1. The data subject has the right to file a complaint with the Authority if he believes that the processing of personal data concerning him by competent authorities for the purposes referred to in article 43 violates his rights. This does not apply to the processing of personal data by judicial and prosecutorial authorities, when they process such data in the context of their judicial function and judicial duties. The Authority informs the data subject of the progress and outcome of the complaint and of the possibility of filing an annulment request before the Council of State against the decision on his complaint, in accordance with article 20."
e) In the third paragraph of Article 71 of Law 4624/2019, on discrimination of personal data and verification of their identity, the word "public" is replaced by the word "competent" and Article 71 is formulated as follows:
"Article 71 Discrimination of personal data and verification of their identity (Article 7 of the Directive)
When processing, the controller distinguishes, as far as possible, between personal data based on factual situations and those based on personal assessments. For this purpose, the controller identifies evaluations based on personal judgments as such, to the extent possible in the context of said processing. It must also be possible to determine which competent authority holds the records on which the assessment is based on personal assessment.'

Article 37

Replacement of title of Section II of Chapter D of Law 4624/2019
The title of Section II of Chapter D of Law 4624/2019 (A' 137) is replaced as follows:
"LEGALITY OF PROCESSING".

Article 38

Legality of processing Addition of Article 45A to Law 4624/2019 (Article 8 of Directive 2016/680)
After article 45 of Law 4624/2019 (A' 137), article 45A is added as follows:
"Article 45A Lawfulness of processing (Article 8 of the Directive)
1. The processing of personal data is lawful only if it is based on the law or the law of the Union and is necessary for the performance of a task carried out by the competent authorities for the purposes provided for in article 43.

2. The special arrangements under par. 1 which include the legal basis for the processing by the competent authorities for the purposes defined in article 43, define at least the purposes of the processing, the personal data processed and the purposes of processing, the procedures for maintaining the integrity and confidentiality of personal data, as well as the competent authority or authorities, by virtue of the duties assigned to them by law, to carry out this processing."

Article 39

Processing of special categories of personal data Replacement of article 46 of Law 4624/2019

Article 46 of Law 4624/2019 (A' 137) is replaced as follows:

"Article 46 Processing of special categories of personal data (Article 10 of the Directive)

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the exclusive identification of a natural person or data relating to health or sexual life or sexual orientation, are permitted only when they are absolutely necessary to achieve the purposes of Article 43 and provided that: a) they are expressly provided for by law or Union law and b) they are imposed for the protection of vital interests of the data subject or another natural person, or c) this processing concerns data that has been manifestly made public by the data subject.

2. When the processing concerns the special categories of data in paragraph 1, appropriate safeguards are applied to protect the data subject, such as:

a) specific specifications and requirements for security and for processing control, b) specific and short deadlines within which the necessity of the further observance of said data is reviewed and documented, c) measures to raise the awareness of persons involved in the processing of data, d) restrictions on access to said data within the competent authority, e) maintenance and processing of special categories of data in a manner distinct from the processing of other categories of data, f) pseudonymisation of personal data belonging to the special categories, if this does not prevent the achievement of the purpose of the processing, g) encryption of the data, h) special procedural arrangements that ensure the legal processing and the protection of the rights of persons in case of transmission or processing of such data for other purposes."

Article 40

Processing for other purposes Amendment of article 47 of Law 4624/2019

The second paragraph of Article 47 of Law 4624/2019 (A' 137) is repealed and Article 47 is amended as follows:

"Article 47 Processing for other purposes (articles 4 and 9 par. 1 of the Directive)
The processing of personal data for a purpose other than that for which they were collected is permitted if the other purpose is one of the purposes referred to in Article 43, the controller is authorized by law to process data for this purpose and the processing carried out is necessary and proportionate to this purpose."

Article 41

Consent of the subject Replacement of article 49 of Law 4624/2019
Article 49 of Law 4624/2019 (A' 137) is replaced as follows:
"Article 49 Consent of the subject
1. When the processing is based on the consent, in accordance with an express provision of law, of the data subject or concerns measures which, according to the law, the subject himself is entitled to request, the controller is able to demonstrate that the data subject consented to the processing of personal data or requested measures involving such processing.
2. Before giving consent, the data subject is informed about the purpose of the processing, the type of personal data subject to processing and especially in the case that the processing concerns special categories of data, the controller, the expected duration of it and the usual recipients of the data. The data subject is also informed of the legal consequences of consent or not providing it, as well as the right to withdraw it.
3. The consent of par. 1 is a clear, specific, written and free of defects declaration of will, with which the data subject declares that he agrees to be the object of processing the personal data concerning him. Consent is considered valid only when it is based on the subject's free decision. To establish the free will and declaration of the subject, the conditions and circumstances under which it was given are evaluated.
4. The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of processing that was based on consent prior to its withdrawal.
5. If the data subject's consent is provided in the context of a written statement, which also concerns other matters, the request for consent shall be submitted in a way that is clearly distinguishable from the other matters, in an understandable and easily accessible form, using simple wording.
6. If it concerns the processing of special categories of data, the consent is expressly referred to the special category of data.'

Article 42

Automated individual decision-making Replacement of article 52 of Law 4624/2019
Article 52 of Law 4264/2019 (A' 137) is replaced as follows:

"Article 52 Automated individual decision-making (Article 11 of the Directive)

1. It is prohibited to take a decision based solely on automated processing, including profiling, which produces adverse legal effects for the data subject or significantly affects him, unless expressly provided for by a statutory provision or Union law, which defines the appropriate guarantees for the rights and freedoms of the data subject and, as a minimum, includes arrangements guaranteeing the specific and indecipherable information of the data subject, the right to ensure human intervention on the part of the data controller and the right of the data subject to formulate his views, to demand justification of the decision taken following said assessment and to challenge or request a review of the decision.

2. The decisions of paragraph 1 may not be based on the processing of the special categories of personal data referred to in paragraph 1 of article 46, unless this is expressly provided for by a provision of law or by Union law and there are appropriate measures for the protection of the rights, freedoms and legal interests of the data subject, including the safeguards defined in paragraph 2 of article 46.

3. It is prohibited to draw up a profile that results in discrimination against natural persons based on the special categories of personal data referred to in paragraph 1 of article 46."

Article 43

Correction of personal data Storage and review deadlines Limitation of processing Replacement of article 73 of Law 4624/2019

Article 73 of Law 4624/2019 (A' 137) is replaced as follows:

"Article 73 Correction of personal data Storage and review periods Limitation of processing (Article 5 of the Directive)

1. The controller corrects inaccurate personal data.

2. The data controller deletes the personal data without delay if their processing is unlawful and they must be deleted to fulfill a legal obligation or their knowledge is no longer necessary to fulfill the purposes of the processing.

3. The law determines the storage period. At the end of this period, the data is deleted.

4. The law may provide for the periodic review of the storage period by the controller, the review periods and criteria. The review in question is based on the principle of limiting storage for as long as is necessary to achieve the purpose of the processing defined in par. 2 of article 45A. The criteria, which are taken into account when determining the initial storage period and the periodic review of the necessity of data retention, include, in particular, the category of the data subject, in accordance with Article 70, the age of the subject, the seriousness of the criminal offense and the corresponding criminal sanction, the seriousness of the risk or

potential threat to public safety, the existence of pending criminal investigations, the possible statute of limitations, recidivism and the need to protect victims.

5. The data protection officer participates in the process of reviewing the necessity of further retention of personal data.

6. Paragraphs 3 to 5 of article 56 are applied accordingly. The recipient is also informed if inaccurate personal data has been transmitted or if the personal data has been transmitted illegally.

7. The person in charge of processing ensures compliance with the requirements herein already during the planning of the relevant processing and the corresponding systems and procedures as defined in article 69."

Article 44

Repealed provisions Replacement of article 84 of Law 4624/2019

Article 84 of Law 4624/2019 (A' 137) is replaced as follows:

"Article 84 Law 2472/1997 (A' 50), on the protection of the individual from the processing of personal data, is repealed, subject to paragraph 3 of article 13, the recommendation of the Authority with paragraph 1 of article 15 , of paragraphs 2 and 3 of article 18 and article 21, regarding the imposition of administrative sanctions, in accordance with paragraph 4 of article 13 of Law 3471/2006 (A' 133), which are kept in force."

Article 45

Disclosure of personal data by the prosecution authority Addition of Article 84A to Law 4624/2019

Article 84A is added to Law 4624/2019 (A' 137) as follows:

"Article 84A Disclosure of personal data by the prosecution authority

1. By order of the competent First Instance Prosecutor or the Appellate Prosecutor, if the case is pending before the Court of Appeal, the Greek Police shall make public, for a period not exceeding six (6) months, the details of the identity, image and criminal prosecution of a person accused or convicted of a felony, for a misdemeanor of the Nineteenth Chapter, on crimes against sexual freedom and economic exploitation of sexual life, of the Criminal Code (law 4619/2019, (A' 95), as well as for a misdemeanor punishable with a prison sentence of at least two (2) years.

2. The disclosure of the personal data of par. 1 aims exclusively to:

a. in the investigation, detection or prosecution of the crimes of paragraph 1,

b. in the execution of an arrest warrant or conviction of the accused or convicted person for the crimes of par. 1.

3. The competent prosecuting authority may issue a specifically and thoroughly reasoned order, as long as the disclosure, in whole or in part, of the personal data of the accused or the convicted person referred to in par. 1 is suitable for achieving the purposes of par. 2 and to prevent a threat to public security in relation to the crime under investigation and it is not possible to choose other measures less burdensome to fundamental rights.

4. The application is submitted by the competent authorities of paragraph n of article 44. In case of a preliminary investigation, the application is submitted by the competent investigative officer, while in the case of a main investigation by the investigator. The order of the prosecuting authority, which is executed by the Greek Police, contains: a) the identity details of the accused or convicted person, b) his image, c) the criminal prosecution or conviction, as well as the citation of the necessary facts, d) the purpose and objective of the disclosure, e) the manner and means thereof, f) the time period for maintaining the disclosure and any reproduction thereof, within the framework of par. 1.

5. The disclosure of personal data, which pertains to criminal prosecution or conviction, takes place in a manner consistent with the obligation to respect the presumption of innocence. The validity of the provision automatically ceases with the expiry of the specified period of time and the preservation of the publicized personal data, as well as any reproduction thereof, is prohibited. In case of fulfillment of the intended purpose and objective in a shorter period of time than that of par. 1, the public prosecutor revokes the provision by issuing a new one, which is executed by the Hellenic Police.

6. An appeal against the order of the public prosecutor is allowed within two (2) days from the notification to the accused or convicted person before the Head of the First Instance Prosecutor's Office or the Head of the Appellate Prosecutor's Office, if the case is pending before the Court of Appeal, which decides within two (2)) of days. Until the competent Prosecutor decides, the execution of the order and the publication of personal data are prohibited.

7. Exceptionally, in the felonies of articles 187, on criminal organization, 187A, on terrorist acts-terrorist organization, 187B, on criminal support and those of the Nineteenth Chapter, on crimes against sexual freedom and economic exploitation of sexual life Criminal Code, the prosecutor's order is executed immediately, and it is validated by the head of the Appellate Prosecutor's Office within twenty-four (24) hours, if it has been issued by the First Instance Prosecutor. Otherwise, the validity of the relevant provision automatically ceases at the end of the twenty-four (24) hour period."

Article 46

Establishment of a Permanent Scientific Committee on Personal Data

1. A Permanent Scientific Committee on Personal Data is established in the Ministry of Justice.

2. The Commission's mission is to carry out law-making tasks, after monitoring scientific and jurisprudential developments and the national and EU legal framework for the protection of personal data and participation in relevant international bodies.

3. The Committee may participate, without the right to vote, if invited by it, employees and executives employed with any type of relationship in public or private sector entities, including independent authorities, with a subject related to the processing of personal data.

4. The Committee has seven members and is made up of persons with professional and scientific experience in the field of personal data. The President of the Commission is appointed a senior or senior judicial officer.

5. The President and the members of the Committee, together with an equal number of substitute members, as well as the Secretary of the Committee are appointed by a decision of the Minister of Justice, which is published in the Government Gazette.

6. No compensation shall be paid to the President, the members and the Secretary of the Committee, apart from travel expenses, daily out-of-office compensation and overnight expenses.

CHAPTER G' : UTHORIZING, FINAL, TRANSITIONAL AND REPEAL PROVISIONS

Article 47

Authorizing provisions

1. By joint decision of the Governor of E.Y.P. and of the Minister of Justice, which is not published in the Government Gazette, defines the technical and procedural details for the implementation and operation of the E.Y.P.'s electronic platform. provided for in par. 3 of article 8 and the general observance of the procedure for the delivery of the provisions according to par. 1 and 2 of article 8. Until the decision of the first paragraph is issued, as well as in an extremely urgent or unforeseen need, the excerpt or the entire arrangement is delivered with a receipt in a closed envelope and received by specially authorized personnel.

2. By a joint decision of the Ministers of Citizen Protection and Justice, which is not published in the Government Gazette, the technical and procedural details for the implementation and operation of the DAEEB electronic platform are determined. provided for in par. 3 of article 8 and the general observance of the procedure for the delivery of the provisions according to

par. 1 and 2 of article 8. Until the decision of the first paragraph is issued, as well as in an extremely urgent or unforeseen need, the excerpt or the entire arrangement is delivered with a receipt in a closed envelope and received by specially authorized personnel.

3. By a joint decision of the Ministers of Justice and Digital Governance, which is not published in the Government Gazette, the technical and procedural details for the implementation and operation of the procedure regarding the delivery, by electronic encrypted message, of the extract or the whole order or the will respectively, which are issued for the verification of the crimes of article 6. Until the decision of the first paragraph is issued, as well as in extremely urgent or unforeseen need, the excerpt or the entire order or the will is delivered with proof in a closed file and are received by specially authorized personnel.

4. With a presidential decree, issued within three (3) months from the entry into force of this, following a proposal by the Ministers of Citizen Protection, National Defence, Justice and Digital Governance, the conditions under which it is permissible to enter into contracts from part of state structures for the supply of software or monitoring devices of article 370F of the Criminal Code for the fulfillment of their purposes.

5. By joint decision of the Minister of Finance and the person responsible for the supervision of the E.Y.P. of a member of the Government, compensation may be provided for public officials, employees and all types of executives employed in the public sector, for private experts and for members of the working groups of article 24, in derogation of the applicable provisions on remuneration or compensation due to participation in public sector boards and commissions.

6. By decision of the Minister of Digital Governance, after a recommendation from the National Cybersecurity Authority, the terms, conditions, as well as any other necessary details are determined in relation to the participation in the SOC National Network of article 31 and other entities that provide cybersecurity services and are active in the field of cyber security.

7. For the application of article 31 and others by decision of the Minister of Digital Governance, which is not published in the Government Gazette, after a recommendation from the National Cybersecurity Authority, the architecture and the more specific functional and technical requirements and specifications of the infrastructure of the Unified SOC and sectoral SOCs, with the aim of meeting the highest security standards and ensuring, in particular, joint situational awareness, interoperability, sharing of tools and platforms, fuller and faster exchange of information and appropriate quality data, implementation of principles of security by design and by default and privacy by design and by default. With a similar decision, following a proposal from the National Cyber Security Authority, the types of data, which are

processed and shared by the SOC National Network, the procedures for preventive controls, the details of the support of the agencies, the procedures for reporting and dealing with incidents and any other necessary detail for the implementation of this.

Article 48

Final provisions

1. Paragraph 1 of article 36 of the Code of Criminal Procedure (law 4620/2019, A' 96), on the powers of economic crime prosecutors, and paragraph 1 of article 17 of law 4786 are not affected by the application of this /2021 (A' 43), on the powers of the European Public Prosecutors.

2. Where provisions of the current legislation are referred to in articles 3, 4 and 5 of Law 2225/1994 (A' 121), a reference to the relevant provisions herein is understood.

3. With the entry into force of this, the serving Deputy Commanders of the National Intelligence Service (NIS) are automatically terminated. Until the appointment of Deputy Governors, pursuant to paragraph 4 of article 9 of Law 3649/2008 (A' 39), as replaced by paragraph 2 of article 18 hereof, their powers shall be exercised by the Governor of E. H.P..

Article 49

Transitional provisions

Until the issuance of the decisions of articles 32 and 33 hereof, the provisions set forth in no. 1027/4.10.2019 decision of the Minister of State (B' 3739).

Article 50

Repealed provisions

Removed:

1. Articles 3, 4, 5 and 7 of Law 2225/1994 (A' 121), on the lifting of confidentiality.

2. The second and third paragraphs of para. b of par. 1 of article 5 of Law 3649/2008 (A' 39), on the approval of the order to lift confidentiality.

3. The last paragraph of par. 1 of article 39 of Law 3959/2011 (A' 93), regarding the submission of a request for the lifting of confidentiality by the Competition Commission.

4. Paragraph d of paragraph 3 of article 93 of Law 4099/2012 (A' 250), paragraph g of paragraph 3 of Article 36 of Law 4443/2016 (A' 232) and paragraph h of paragraph 4 of article 67 of Law 4514/2018 (A' 14), regarding the submission of a request for the lifting of confidentiality by the Capital Market Commission.

5. Paragraph 4 of article 10 and paragraph 3 of article 12 of Law 4577/2018 (A' 199), on authorizing provisions for cybersecurity issues.

CHAPTER H': COMMENCEMENT OF EFFECTIVENESS

Article 51

Start of force

1. Without prejudice to par. 2, the validity of this law begins from its publication in the Government Gazette, unless otherwise provided in the individual provisions.

2. The validity of article 27 starts from 1.4.2023.

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

Athens, December 9, 2022

The President of the Republic
KATERINA SAKELLAROPOULOU

The Ministers
Finance CHRISTOS STAIKOURAS
Deputy Minister of Finance THEODOROS SKYLAKAKIS
Development and Investments SPYRIDON ADONIS GEORGIADIS
Foreign Affairs NIKOLAOS GEORGIOS DENDIAS
Deputy Minister of Foreign Affairs MILTIADIS VARVITSIOTIS
of National Defense NIKOLAOS PANAGIOTOPOULOS
of Labor and Social Affairs KONSTANTINOS HATZIDAKIS
Health ATHANASIOS PLEURIS
of Environment and Energy KONSTANTINOS SKREKAS
Protection of the Citizen PANAGIOTIS THEODORIKAKOS
Justice KONSTANTINOS TSIARAS
Interior MAVROUDIS VORIDIS
Deputy Minister of the Interior STYLIANOS PETSAS
Maritime and Island Policy IOANNIS PLAKIOTAKIS
of Climate Crisis and Civil Protection CHRISTOS STYLIANIDES
State GEORGIOS GERAPETRITIS
State KYRIAKOS PIERRAKAKIS
Deputy Minister to the Prime Minister IOANNIS ECONOMOU
The Great Seal of the State was considered and affixed.

Athens, December 9, 2022

The Acting Minister of Justice

KONSTANTINOS TSIARAS