Law Enforcement Directive Implementation Country Report: Greece

Eleftherios Chelioudakis

EDRi
European Digital Rights

Law Enforcement Directive Implementation Country Report: Greece

Eleftherios Chelioudakis, August 2024

TABLE OF CONTENTS

1. Introduction – The transposition of the LED into the Greek legal framework

The Greek Data Protection Act (GDPA), known as Law 4624/2019, enforces the General Data Protection Regulation (GDPR) and transposes the Law Enforcement Directive (LED) into the Greek legal framework. Specifically, Articles 1-42 of the GDPA enforce the GDPR, while Articles 43-82 transpose the LED.

However, it is crucial to highlight early on that the transposition of the LED into the Greek legal framework presented a series of problems. To begin with, although Article 63 of the LED required Member States to adopt and publish, by 6 May 2018, the laws, regulations, and administrative provisions necessary to comply with this Directive, the Greek state did not meet this deadline. Consequently, the European Commission launched a formal notice to Greece in July 2018 (European Commission, 2018). Moreover, the Greek civil society organisation (CSO) Homo Digitalis lodged a complaint in May 2019 before the European Commission against Greece for non-compliance with EU law (Homo Digitalis, 2019a). Two months later, in July 2019, the European Commission decided to refer Greece to the Court of Justice of the EU (CJEU) for failing to transpose the LED (European Commission, 2019).

This referral compelled the Greek state to act swiftly to avoid financial sanctions from the CJEU, resulting in the adoption of Law 4624/2019 within just one month (August 2019).

1.1 CSO concerns about LED transposition

The provisions of the new GDPA transposing the LED nevertheless appeared to raise challenges. These were first highlighted in a report published by civil society and academics in Greece (Homo Digitalis, 2019b), the same month the GDPA was adopted. In September, civil society actors expressed similar concerns before the Hellenic Data Protection Authority (HDPA), requesting it to issue an opinion on the matter (Homo Digitalis & EKPIZO, 2019). Additionally, a new complaint was filed with the European Commission, claiming that the provisions of Law 4624/2019 did not comply with the LED (Homo Digitalis, 2019c). The main concerns raised by civil society actors before the Hellenic DPA and the European Commission were the following:

- **Art. 5 of the LED:** According to the CSOs, Art. 73 of the Greek Law, which was supposed to implement Art. 5 LED (according to its own title) neither provided for time limits to be established for the erasure of personal data, nor for a periodic review of the need for the storage of personal data by Greek law enforcement authorities.
- **Art. 11 of the LED**: While Art. 52(1) of the Greek Law stated that a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is allowed only when it is authorised by law, according to the CSOs it did not state that such a law shall provide appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.
- **Art. 32(4) of the LED:** According to the CSOs, Art. 6(5) of the Greek Law gave Greek national authorities neither the option to publish the contact details of their data protection officer nor to communicate these details to the Greek supervisory

authority. The Greek legislator based this decision on reasons linked to national security and confidentiality obligations

- **Art. 55 LED:** According to the CSOs, the Greek Law deprived people of all of the rights provided for in Art. 55 LED, since it did not cover any of them. More precisely, data subjects in Greece do not, under the Greek Law 4624/2019, have the right to mandate a not-for-profit body, organisation or association (one that has been properly constituted in accordance with Greek law, has statutory objectives which are in the public interest, and is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data) to lodge the complaint on their behalf, and to exercise the rights referred to in Art. 52, 53 and 54 LED on their behalf.
- **Art. 49 GDPA**: This article provided consent as a legal basis for the data processing activities of law enforcement authorities. According to the CSOs, this provision was in conflict with the rationale of the LED as well as with Recitals 35 and 37 LED, while it contradicted Article 29 Working Party Opinion WP258 (29.11.2017, p. 9).

1.2 The Hellenic DPA and the European Commission step in

The purpose of this sub-section is to provide a comprehensive overview of the Greek government's past shortcomings in transposing the LED into national law. Despite receiving numerous recommendations from the Hellenic Data Protection Authority (HDPA) and the European Commission, Greece has consistently failed to address key issues in its legislative framework. This analysis highlights that, even after these interventions, the legal provisions in place today remain weak in several critical areas, reflecting a persistent lack of alignment with the Directive's requirements.

The Hellenic DPA responded promptly to the CSOs' request mentioned in the previous sub-section, and in January 2020 issued Opinion 1/2020 (Hellenic Data Protection Authority, 2020a). Based on the DPA's Opinion, "(i)n several cases, a series of provisions of the Directive have not been incorporated at all; in other cases, the text of the Directive has been transferred verbatim without adaptation to national legislation; while in some cases, the transposition is incorrect" (p.21). Regarding specific articles, the Hellenic DPA highlighted the following:

- **Article 43 GDPA:** Article 1(2)(a) of the Directive has not been transposed, while Article 1(1) has been partially transposed. The DPA stated that the objective of the LED, which is the protection of data processed for the purpose of prosecuting a crime, is not clearly stated.
- **Article 44 GDPA:** The DPA highlighted that Article 3(7)(a) of the LED, which concerns the definition of the "competent (public) authority", has not been incorporated into the Greek Act. In the context of a proper incorporation, the specific authority responsible for monitoring the application of the LED should have been defined, as being the Data Protection Authority.
- **Article 47 GDPA:** According to the DPA, this provision exceeds the legitimate purpose of data collection and processing within the scope of the LED, and it is not in compliance with Recital 29 and Article 4 LED.
- **Article 51 GDPA:** According to the DPA, this article is not related to the LED's transposition, because it provides that people involved in the data processing activities of Law Enforcement Authorities (LEAs) shall have an authorisation to do

so. Yet no specific guidance is provided with regard to this authorisation, and according to the DPA, this provision is vague.

- **Article 52 GDPA:** According to the DPA, Article 11(1) of the LED has been inadequately transposed, because Article 52 omits the reference to "appropriate safeguards" required by the LED to protect the rights and freedoms of the data subject, including at least the right to obtain human intervention from the data controller. Moreover, the wording from Article 11(2) of the Directive regarding "appropriate measures" is merely repeated, and the national legislator has not specified or defined the relevant criteria in accordance with Recital 33 of the LED.

- **Article 67 GDPA:** The Greek act provides that in the context of the procedure of "prior consultation with the DPA"(Article 28 LED), if the proposed processing is necessary for the performance of the controller's duties and, as such, is particularly urgent, the controller may proceed with the processing after the consultation has started. According to the Greek DPA, this option is compliant with Article 28 LED.

- **Article 70 GDPA:** According to the DPA, this article transposes Article 6 LED and distinguishes between different categories of data subjects, without providing specific details for vulnerable groups, such as children. Additionally, it does not address the implications for personal data processing operations in the context of different categories of data processed (e.g., maintenance in different files, impact on data retention periods, destruction under various conditions, etc.).

- **Article 73 GDPA:** This article transposes Article 5 LED, but according to the DPA, it only makes general references to retention periods or periodic review, without specifying concrete criteria in accordance with Recital 33 LED.

- **Article 74 GDPA:** This article transposes Article 25 LED (logging), but according to the DPA, it does not provide for the possibility of retaining logging details until the completion of DPA's investigatory activities.

The European Commission also responded to the CSOs' request, and in June 2020 it initiated a procedure with the Hellenic Government (Homo Digitalis, 2020a). This procedure lasted almost two years and concluded in April 2022, with the European Commission sending the Hellenic Government a letter under protocol number INFR (2022)2021C(2022)1666. The specific content of the European Commission's letter was not made public, but the Hellenic DPA highlighted in its Opinion 5/2022 that "the European Commission in the (2022)2021C(2022)1666 warning letter, which was issued following the examination of a complaint regarding potential issues with the compliance of Law 4624/2019 with the Law Enforcement Directive, determined **that Greece had violated its obligations under Article 2, paragraph 1, paragraphs 5, 8, and 11, and Article 32, paragraph 4 of the Directive**. (...) In the same letter, the European Commission reserved the right to issue a reasoned opinion for referring the matter to the Court of Justice of the European Union" (Hellenic Data Protection Authority, 2022a, p.2).

1.3 The revised Greek Data Protection Act

Following these developments, the Hellenic Government initiated a revision of Law 4624/2019 in November 2022 and adopted Law 5002/2022 in December 2022, which revised a set of provisions related to the LED's implementation. Thus, the analysis provided in this document reflects the latest version of Law 4624/2019, as revised by Law 5002/2022 in December 2022.

2. The rights of the Data Subject

2.1 Restrictions

Articles 53 to 59 of the GDPA deal with data subjects' rights and related restrictions. The following sections provide an analysis of the GDPA's related articles implementing Articles 12 to 16 LED.

2.1.1 Article 12 LED

To begin with, Article 53 GDPA, according to its own title, transposes Article 12 LED (and Article 13 LED – see below). The article reads as follows:

> The controller shall provide general and easily accessible information to the public in plain and intelligible language through the website of the competent authority with regard to: (a) the purposes of processing, (b) the right of the data subject to request from the controller access to, rectification, erasure or restriction of processing, (c) the identity and the contact details of the controller and the DPO, (d) the right to lodge a complaint with the Authority, and (e) the contact details of the Authority.[1]

Moreover, Article 57 GDPA, according to its own title, also transposes Article 12 LED. The article reads as follows:

> 1. The controller shall communicate with the data subject in a concise, intelligible and easily accessible form, using clear and plain language, in particular when addressing minors. The information shall be provided without prejudice to specific provisions by any appropriate means, including by electronic means. The controller should provide the information in the same form as the request. 2. Without prejudice to Article 55(5) and Article 56(6), the controller shall without delay inform the data subject of the status of his or her request. 3. The information provided in accordance with Article 53, any communication made in accordance with Articles 54 and 64, as well as the requests processed in accordance with Articles 55 and 56, shall not be subject to a fee. Where a request in accordance with Articles 55 and 56 is manifestly unfounded or is being abused, the controller may charge a reasonable fee based on administrative costs or may refuse to act on the request. In this case, the controller must be able to demonstrate the manifestly unfounded or excessive character of the request. 4. Where the controller has reasonable doubts concerning the identity of the data subject making the request referred to in Articles 55 and 56, the controller may request the provision of additional information necessary to confirm the identity of the data subject.[2]

When the wording of Article 12 LED is taken into consideration, it appears from the above provisions of Articles 53 and 57 GDPA that Article 12 LED has been transferred verbatim without adaptation to national legislation:

[1] This is the Hellenic DPA's English translation of Law 4624/2019. The word "competent" has replaced the word "public" following the revisions put forward by Law 5002/2022. This is the author's own translation of the Greek word "αρμόδια", which replaced the Greek word "δημόσια". See more in the Glossary section.
[2] This is the Hellenic DPA's English translation of Law 4624/2019. See more in the Glossary section.

- The Greek framework repeats, in Article 57(1) and in a slightly loose manner, the wording of Article 12 LED, allowing the controller to take reasonable steps to provide any information and/or communication in relation to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The article mentions that information shall be provided by any appropriate means, including by electronic means, while a special mention is made to children. Moreover, it is stated that, as a general rule, the controller shall provide the information in the same form as the request.

- The Greek framework repeats, in Article 57(2), the wording of Article 12 LED providing for the controller to inform the data subject in writing about the follow-up to his or her request without undue delay. However, no specific time period specifies the concept of "undue delay".

- The Greek framework repeats word-for-word the text of Article 12(4) and Article 12(5) LED.

2.1.2 Article 13 LED

Article 54 GDPA, according to its own title, transposes Article 13 LED. The article reads as follows:

> 1. In specific cases, and in particular where the personal data of the data subject have been collected in secrecy and in order to enable the exercise of his or her rights, the data subject should, in addition to the information referred to in the previous Article, be informed, at least, of: (a) the legal basis for the processing; (b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period; (c) where applicable, the recipients of the personal data; (d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject. 2. In the cases referred to in the previous paragraph, the controller may delay, restrict or omit the provision of information to the data subject, if necessary, in order to: (a) enable the competent authorities to perform their duties, as described in Article 43, (b) ensure national security or public security, or (c) protect the legitimate interests of third parties, which would otherwise be threatened, if the interest in avoiding these threats overrides the interest of the data subject in being informed. 3. The provisions of paragraph 7 of the following Article shall also apply to the restrictions of the previous paragraph.[3]

When the wording of Article 13 LED is taken into consideration, it appears from the above provisions of Article 54(2) GDPA that:

- While the principle of necessity is specifically mentioned, the principle of proportionality is not. However, the three-part test of legality, proportionality, and necessity is indispensable in evaluating the legitimacy of state-imposed limitations on fundamental rights. Each element of the test is interdependent and serves a distinct purpose in ensuring that restrictions are not only legally grounded but also fair and necessary in a democratic society. Necessity, in particular, cannot exist in a vacuum; it must be understood and applied within the context of legality and proportionality. A measure deemed necessary must first be legally valid and then proportionate to the aim it seeks to achieve. Without the foundation of legality and the balance provided by

[3] This is the Hellenic DPA's English translation of Law 4624/2019. See more in the Glossary section.

proportionality, the concept of necessity loses its meaning and risks justifying excessive or arbitrary restrictions.

- The first of the reasons provided by the GDPA for delaying, restricting or omitting the provision of the information to the data subject is "**enabling"** ("για την εκτέλεση των καθηκόντων των" in the official Greek text of the GDPA) the competent authorities to perform their duties. However, this is not in line with the wording of Article 13 (3)(a) and (b), which specifically mention that such a delay or restriction or omission could take place in order to "**avoid"** ("την αποφυγή της παρεμπόδισης" in the official Greek text of the LED*)* obstructing official or legal inquiries, investigations or procedures or to "**avoid**" prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties. Thus, the exception that the Greek Law provides could be considered as much broader than the wording of the LED. The GDPA, by employing the term "enabling" ("για την εκτέλεση των καθηκόντων των"), introduces a broader scope for justifying the delay, restriction, or omission of information provided to a data subject compared to the LED's use of the term "avoiding" ("την αποφυγή της παρεμπόδισης"). This has significant implications for the balance between individual rights and the operational needs of authorities, as the verb "enabling" implies a proactive facilitation or empowerment of competent authorities in performing their duties. It suggests that any action or decision that contributes to the authorities' ability to execute their responsibilities could justify withholding information from a data subject. This could encompass a wide range of circumstances where authorities believe that providing information could, in any way, hinder their ability to carry out their functions effectively. In contrast, the term "avoiding" carries a more restrictive implication. It specifically targets the prevention of obstructive outcomes – those that directly impede legal inquiries, investigations, or criminal procedures. The focus is on preventing negative consequences that would obstruct the process, rather than broadly ensuring that authorities can perform their duties. Therefore, it is important to highlight that the Greek Law's wording grants broader discretion to authorities. Under the Greek framework, authorities could potentially justify withholding information whenever they deem it necessary to ensure the smooth execution of their duties, even in situations that do not directly relate to ongoing investigations or legal processes. This contrasts with the more narrowly tailored exceptions in the LED, which only permit such actions when there is a clear risk of obstructing or prejudicing specific legal or investigative processes.

- The second reason provided by the GDPA for delaying, restricting or omitting the provision of information to the data subject is to ensure national or public security. Thus, here the GDPA has transposed in a slightly loose manner the wording of Article 13(3)(c) LED (the Greek text does not even have a verb, it merely mentions public and national security, so it could be perceived as a verbatim transfer without adaptation).[4]

- The third reason provided by the GDPA for delaying, restricting or omitting the provision of information to the data subject is to protect the "**legitimate interests**" of third parties ("για την προστασία των έννομων συμφερόντων τρίτων" in the official Greek text of the GDPA). Again, this provision is in contradiction with the wording of the LED, since Article 13(3)(e) specifically mentions "protect the **rights and freedoms of others**" ("την προστασία των δικαιωμάτων και των ελευθεριών τρίτων" in the Greek text of the LED). The term "legitimate interests of third parties" is inherently broader and more ambiguous than the "rights and freedoms of others". While "rights and freedoms" refers to clearly defined and legally protected entitlements under human rights and constitutional law, "legitimate interests" encompasses a wider range of concerns, including economic, business, or even reputational interests of both natural

[4] The Greek text is "για την εθνική ασφάλεια ή τη δημόσια ασφάλεια".

and legal persons. This broader scope allows for a wider range of justifications for withholding information from a data subject, which could dilute the protection of individual rights.

2.1.3 Articles 14 & 15 LED

Article 55 GDPA transposes, according to its own title, Articles 14 and 15 LED. This article states that the data controller may refuse to provide access to the data subject, or restrict such access, in whole or in part and where necessary, for the same reasons provided in Article 54 GDPA.

> 4. In the cases referred to in paragraph 2 of the previous Article, the controller may refuse to provide information in accordance with the first subparagraph of paragraph 1 or to restrict, in whole or in part, the provision of information in accordance with the second subparagraph of paragraph 1.[5]

Thus, the transposition of Articles 14 and 15 LED into Article 55 GDPA poses the same risks analysed in the previous section, since the provided wording (enabling, legitimate interests, etc.) allows for a wider range of limitations on data subject's rights.

2.1.4 Article 16 LED

Article 56 GDPA transposes, according to its own title, Article 16 LED. This article provides for specific limitations with regard to the right to erasure:

> 3. Instead of erasing personal data, the controller shall restrict the processing, where: (a) there is reason to assume that the erasure would compromise the legitimate interests of the data subject, (b) the personal data are to be kept, provided they serve as evidence for the purposes of Article 43, or (c) erasure would be impossible or would involve a disproportionate effort due to the special storage mode.[6]

When the wording of Article 16 LED is taken into consideration, it appears from the above provisions of Article 56 GDPA that:

- The Greek framework **provides for two completely new grounds**, namely Article 56(3)(a) and Article 56(3)(c). On point (a), the provision allowing the denial of a data subject's request for erasure based on the assumption that it would compromise their legitimate interests represents a paternalistic approach that undermines the autonomy and agency of the individual. This provision presumes that LEAs or data controllers are better positioned to determine what is in the best interest of the data subject, thereby overriding the individual's right to make decisions regarding their own personal data. Allowing data controllers to make such determinations introduces a significant risk of misjudgment or abuse. The data controller's interpretation of the data subject's "legitimate interests" may be influenced by factors that do not accurately reflect the individual's intentions or desires. Moreover, this provision could be misused by data controllers to retain data for reasons that ultimately benefit the controller more than the data subject. On point (c), by

[5] See footnote 3
[6] Ibid.

introducing a vague and potentially broad exception based on the "special storage mode", this provision weakens the accountability of data controllers. It provides an easy escape clause that could be used to justify retaining data that should otherwise be erased. Instead of taking proactive measures to ensure data is stored in a manner that allows for its erasure when required, data controllers might use this provision to avoid investing in the necessary technical and organisational measures, thereby evading their responsibility to protect the rights of data subjects and their compliance with the principles of accountability, integrity and confidentiality.

- The ground provided in Article 16(3)(a) LED, namely that "the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained", **is not provided** in the Greek Law.

- The only ground that has been properly transposed is Article 16(3)(b), i.e. that "the personal data must be maintained for the purposes of evidence".

2.2 The exercise of data subject rights in practice

There is not enough data available to reach solid conclusions with regard to the exercise of data subjects' rights in practice in Greece. The Greek Data Protection Authority has been publishing statistical data classifying the complaints received based on the applicable legislation (GDPR, LED, ePrivacy) since October 2020. Before that date, the Greek DPA was only announcing the general number of complaints received, without differentiating between complaints received based on the GDPR, the LED or the ePrivacy Directive. Thus, from October 2020 until April 2024, out of a total of 768 complaints received, only 4 are related to the LED (0,5%), according to data published by the Greek DPA (Hellenic Data Protection Authority 2022-2024).[7] The Hellenic Police is not publishing statistical data with regard to data access requests or other requests received by data subjects (Hellenic Police, 2024).

Based on the above, the only conclusion that can be drawn is that the filing of complaints before the Greek DPA on LED matters remains very limited, and the vast majority of complaints received deal with the GDPR. No information is available with regard to data subjects' requests submitted before the Hellenic Police, since it was not possible to find related data through the Hellenic Police's website (Hellenic Police, 2024).

3. Biometric data and the requirement of strict necessity

To begin with, Article 44 GDPA defines biometric data as "personal data resulting from specific technical processing related to the physical, biological, or behavioural characteristics of a natural person, which allow or confirm the unequivocal identification of that person, such as facial images or fingerprint data".[8]

[7] The DPA publishes statistical data every 3 months. See in detail in the bibliography section.

[8] This is the author's own translation, since there is no unofficial Greek translation provided by the GDPA on the revised provisions of Law 4624/2019. The Greek text of Article 3(13) LED and Article 44 GDPA are identical:
Article 3(13) LED: «βιομετρικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα·
Article 44 GDPA: «βιομετρικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα·

With regard to processing biometric data, or other special categories of data, Article 46 GDPA, according to its own title, transposes Article 10 LED. This is one of the articles that was heavily revised with Law 5002/2022.

The updated version of this article states the following:

> The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership in a trade union, as well as the processing of genetic data, biometric data for the sole purpose of identifying a natural person, or data concerning health or sexual life or sexual orientation, is permitted only when it is absolutely necessary to achieve the purposes of Article 43 and provided that: a) it is explicitly provided for by Greek law or Union law, and b) it is required for the protection of the vital interests of the data subject or another natural person, or c) the processing concerns data that has been manifestly made public by the data subject.[9]

Taking into account the wording of Article 10 LED, it is clear that it has been transferred verbatim into the Greek Law. Specifically, Article 10 LED mentions that the processing of special categories of data is only allowed under three conditions:

(a) where authorised by Union or Greek law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject.

With regard to non-special categories of personal data, Article 45A GDPA states: "The processing of personal data is lawful only if it is based on law or Union law and is necessary for the performance of a task carried out by the competent authorities for the purposes provided in Article 43". Thus, as long as there exists a legal provision that allows for the processing activity, and this processing activity is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security, then data controllers can process this information. Thus, the only legal basis that data controllers can use is, according to Article 45A, Greek or Union law.

However, Article 49 GDPA **allows for the legal basis of consent** to be used for processing both special categories and non-special categories of personal data, but only where national legislation expressly authorises this use.. However, as explicitly stated in Recital 35 LED: "the consent of the data subject as defined in Regulation (EU) 2016/679 should not provide a legal basis for the processing of personal data by competent authorities. Where the data subject is obliged to comply with a legal obligation, he or she does not have a genuine and free choice and, consequently, the reaction of the data subject cannot be considered as a free expression of his or her will". Of course, as the text of the recital underlines, Member States may provide by law that the data subject can agree to the processing of his or her own personal data for the purposes of Directive 2016/680, such as DNA testing in criminal investigations or the surveillance of his or her location with electronic tags for the purpose of executing criminal sanctions. This agreement is not defined as "consent" but as "voluntary agreement" to avoid legal confusion of terminology used (Article 29 Working Party on Data Protection, 2017).

[9] This is the author's own translation, since there is no unofficial Greek translation provided by the GDPA on the revised provisions of Law 4624/2019.

Therefore, Article 49 remains in direct contradiction with the provisions of the LED, as it refers to consent and not to voluntary agreement, legal concepts that are completely different from each other. In addition, as Article 29 Working Party on Data Protection (WP29) explicitly states, the consent of the data subject can in no case in itself constitute a legitimate ground for the processing of special categories of data under the LED. However, Article 49 GDPA states in paragraph 6 that consent can also be used for the processing of special categories of personal data, and is therefore in direct breach of the LED. Voluntary agreement, as mentioned in WP29, can be considered simply as an "additional safeguard" for the processing of special categories of personal data, only in cases where the law provides for processing that is particularly intrusive for the data subject, and it can never be considered as a legal basis. Thus, the concept of "voluntary agreement" should not be confused with the concept of "consent", as is the case in the current Article 49 GDPA.

4. Alignment adopting new laws in accordance with Articles 8 or 10 LED

The GDPA in itself cannot be and is not considered to be a legal basis for data processing operations, but instead sets the framework within which other related pieces of legislation shall operate. Based on desk research, there exists one piece of legislation, related to the processing of personal data by LEAs, which attempts to comply with the LED: the Presidential Decree (PD) 75/2020. This degree provides for the installation and operation of portable and non-portable surveillance systems in public spaces[10] where surveillance is deemed necessary. The installation and operation of such systems is permitted only by state authorities. These public authorities include the Hellenic Police, the Fire Brigade and the Hellenic Coast Guard.[11] The definition of surveillance systems includes the use of cameras (equipped in any vehicle or device, such as drones, body-worn cameras, cameras on sticks, etc.).[12] The purposes for which such systems can be deployed are:

> a) the prevention and suppression of specific criminal acts, such as violent crimes, drug trafficking, etc.;
>
> b) traffic management, the regulation of vehicle traffic, as well as the prevention and management of road accidents.

The installation and operation of such systems is permitted only to the extent necessary and when the above-mentioned objectives cannot be achieved as effectively by lesser means. Notably, regarding the installation and operation of surveillance systems for the prevention

[10] According to Law 3917/2011, on which the PD 75/2020 is based, public spaces are: a) those intended for common use according to the current legislation and city plans; b) open spaces freely accessible to an indefinite number of persons, fenced or not, which are made available for common use in a lawful manner; and c) public transport passenger traffic stations.

[11] Irregular Migration is criminalised in Greece, thus border control authorities impose the LED when investigating an irregular entry (this concerns any person on the move who enters Greece via an irregular migration route). The Fire Brigade can use its powers to investigate related criminal acts on the spot, since an investigation unit exists that interrogates people for fire-related criminal acts.

[12] These surveillance systems can have fixed, rotating or mobile cameras, adapted to fixed or portable bases, transported by vehicles of any kind (i.e. ground, sea or air, manned or not) or by natural persons.

or suppression of crimes, sufficient indications are required that the specifically provided-for offences are committed or will be committed in the specific space (Article 5(1) PD 75/2020). Regarding portable surveillance systems, it is provided that their operation is permitted only in cases where there is an imminent, serious risk that the specifically provided-for offences will be committed (Article 5(3) PD 75/2020).

Moreover, the installation and operation of surveillance systems – fixed, rotating or mobile, in public places and during public outdoor gatherings – is allowed under certain conditions, by means of a special reasoned decision of the competent public authority (Article 6(1) PD 75/2020). In this case, the rapid destruction of the collected data is foreseen, i.e. as a rule within 48 hours from the end of the gathering (Article 6(3) PD 75/2020).

Back in 2021, Homo Digitalis, Reporters United and The Press Project filed a request before the Hellenic Data Protection Authority (HDPA) to investigate at least 64 violations of the provisions of PD 75/2020, concerning the use of portable cameras in public places by the Hellenic Police. In particular, in accordance with the provisions of Article 12(2) PD 75/2020, before the operation of any surveillance system in a public place, the Hellenic Police, as the controller, must issue and notify the decision to operate this system at least on its website, specifying: a) the time of activation; b) the duration of its operation; c) the range of its operation; d) its specific characteristics; and e) the justification of the feasibility of its use.

However, by August 2024, the Hellenic Police had not yet complied with the obligation to publish decisions to operate surveillance systems in public places on its website. On the contrary, in breach of its statutory obligations, the Hellenic Police has consistently confined itself to publishing a simple notice on its website, which indicates only the number of each operating decision, the duration of operation of the surveillance systems and their place of operation in a general and vague manner. In other words, that notice does not communicate the content of the operating decision and does not make any reference to the important information required by Article 12(1) of DP 75/2020, namely the scope of operation of the surveillance system, its specific characteristics and the justification for its use. This last element is particularly important in the context of the principle of lawfulness of processing, as Article 5 PD 75/2020 requires that there are sufficient indications that specific criminal offences are being or will be committed in the public place in question, and that there is reasonable belief that there exists a serious risk to public security.

Moreover, the Hellenic Police denied access to these operating decisions even after Homo Digitalis and other citizens filed access to documents requests in December 2020 (Hellenic Police, 2021).[13] Therefore, it appears that the Hellenic Police treats these operating decisions as confidential documents, since they do not publish the decision on their website, and they do not allow access to them to any citizen, a practice that could contradict the provisions of Article 12(2) PD 75/2020. Homo Digitalis maintains that these practices are illegal and undermine the protection of personal data and the relevant safeguards provided for in the PD 75/2020 (Homo Digitalis 2021).

Last but not least, it is important to highlight that there exists a law in Greece that deals with the use of AI systems by public and private entities (Law 4961/2022), but law enforcement is outside of its scope.[14]

[13] The Hellenic Police stated in its reply that the applicants' requests for access to the recorded information cannot be satisfied, as the fulfillment of this right requires the existence of a legitimate interest, which is not discernible on the applicants' part, as there does not appear to be a specific, personal legal relationship connected to the content of the administrative records to which access is being requested.

[14] For more information, see: https://www.kodiko.gr/nomothesia/document/810877/nomos-4961-2022.

5. New Technologies & Big Data

5.1. AI monitoring tool for social media platforms and instant messaging applications

In February 2022, the Hellenic Coast Guard (HCG) published a tender call for the acquisition of a social media monitoring tool. The cost of the project is more than €726,000 (including VAT), partially funded by the Internal Security Fund (Ministry of Shipping and Island Policy of the Hellenic Republic, 2022).

The software will support the HCG's surveillance and migration prediction practices on Facebook, Twitter, VK, Xing, and Instagram, while some of the envisaged features include the collection, analysis and storage of data publicly displayed on these platforms, such as lists of contacts, posts made (including images, videos, comments and reactions), and account information (past and current employment status, past and current residences, past and current education, etc.). Thus, even special categories of personal data could be included in the aforementioned data processing activities on social media and instant messaging applications. Also, the software should allow for the creation of bots that would be able to monitor group conversations in instant messaging applications (the tender makes specific reference to Telegram) for chat-groups of up to 10,000 participants. Such bots would collect the full content of each group conversation (text and photos or other material shared in them), while simulating human activity in order to avoid account blocking by the platform (Ministry of Shipping and Island Policy of the Hellenic Republic, 2022). The Greek company BYTE, jointly with the Greek company GRIVAS, was awarded the contract for this tool (Hellenic Republic, 2022). Based on an interview conducted with Homo Digitalis representatives, and a meeting that took place between Homo Digitalis and the Hellenic Data Protection Authority in December 2023, this tool is not yet deployed by the Hellenic Coast Guard.

In February 2022, a coalition of civil society organisations composed of Homo Digitalis, Privacy International, the Hellenic League for Human Rights, HIAS Greece, and including researcher Phoebus Simeonidis, collectively submitted a request before the Hellenic Data Protection Authority to investigate this project and assess its compliance with the applicable rules on data protection. Following up on this request, the Hellenic DPA informed the coalition that it launched an investigation of this project (Homo Digitalis, 2022a). Originally, there was limited transparency with regard to the progress of the case. However, after one year, the Hellenic DPA officially informed Homo Digitalis that it was investigating the case since the very beginning, and was close to concluding its assessment (Homo Digitalis, 2023 and Zafeiropoulos, 2023).

It is unclear whether the Hellenic Coast Guard has conducted a Data Protection Impact Assessment (DPIA) or consulted with the Hellenic DPA on this matter. The obligation to conduct a DPIA is provided in Article 27 of the Law Enforcement Directive, which states: "Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller

to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data." (Art. 27(1) LED).

In addition, this assessment is to contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the LED, taking into account the rights and legitimate interests of the data subjects and other persons concerned (Art. 27(2) LED). Moreover, according to Article 28 LED, the data controller or processor shall consult the supervisory authority prior to processing: (a) if the DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or (b) if the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects (E. Chelioudakis, 2024).

5.2. Smart Policing system allowing the use of Facial Recognition and Fingerprint Identification Technology during police stops

In 2019, the Greek police signed a €4 million contract for a smart policing project with Intracom Telecom, a global provider of telecommunications systems and solutions. According to the press release of the Greek police, 75% of the project is financed by the European Commission's Internal Security Fund (ISF) 2014-2020 (E. Chelioudakis, 2020).

This smart policing project is composed of portable gadgets enabling the use of Facial Recognition and Automated Fingerprint Identification technologies during police stops. More precisely, police officers will be able to use these gadgets during police stops in urban environments to take a close-up photograph of an individual's face and collect their fingerprints (Hellenic Police, 2018). Then, the fingerprints and photographs collected will immediately be compared with data already stored in national, EU, and third countries' databases for identification purposes, such as SIS II, VIS and EURODAC (Hellenic Police, 2018). The tender call mentions databases held by Europol, international organisations like Interpol, and even databases of third-country institutions, like the FBI (Hellenic Police, 2018).

The police is presenting this project as a more "efficient" way of identifying undocumented or improperly documented migrants living in the country, in comparison to the current procedure, which is to bring any individuals who do not carry identification documents to the nearest police station (Human Rights Watch & Homo Digitalis, 2022). It should be noted that, based on reports published by Human Rights Watch, it is usual practice of the Hellenic Police to conduct massive police stops and identity checks in order to verify the legal status of individuals presumed to be irregular migrants. Thus, it seems likely that the development and deployment of the aforementioned smart policing tools could especially impact migrant communities in urban centres, such as Athens (Human Rights Watch, 2013). It is therefore clear that one of the main target groups of this technology is (perceived) migrants staying in Greece in an irregular manner. The devices were delivered to the Hellenic Police in September 2021, with no information available since then with regard to their deployment (Ministry of Citizen Protection, 2021).

Homo Digitalis was the first to report on this case in a joint research project with AlgorithmWatch, published back in December 2019 (Homo Digitalis, 2019d). The same month, Homo Digitalis submitted a request to access documents before the Hellenic Ministry of Citizens Protection, in charge of the Hellenic Police. With this action, Homo Digitalis

attempted to receive clarification on whether the Hellenic Police had conducted a DPIA, as well as to obtain more information on the legal basis that the Hellenic Police planned to use in the context of the related data processing activities (Homo Digitalis, 2019d). However, the response from the Hellenic Police did not shed light on the questions posed by Homo Digitalis, since it neither confirmed nor denied that a DPIA had been conducted, nor did it make any specific reference to the legal basis upon which the Hellenic Police would base the processing of biometric data (Homo Digitalis, 2020b). Due to this lack of transparency, in March 2020, Homo Digitalis filed a request before the Hellenic Data Protection Authority (HDPA) to investigate the case (European Digital Rights, 2020). The HDPA has accepted the request and, since August 2020, has an open investigation on this matter, which is still ongoing (Hellenic Data Protection Authority, 2020b) while a decision is anticipated (Hellenic Data Protection Authority, 2022b). Such an extensive delay could raise questions about the efficiency of the HDPA's oversight mechanism, and thus its compatibility with EU law standards.

Based on the email communications shared by the HDPA with Homo Digitalis in the context of this investigation, the Hellenic Police had not originally conducted a DPIA, and had held no prior consultations with the HDPA (E. Chelioudakis, 2024).

Finally, the Hellenic Police appear to have failed to establish a clear legal basis for the processing of special categories of personal data in the context of this tool. According to Article 10 of the Law Enforcement Directive, processing of biometric data for the purpose of uniquely identifying a natural person "shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject". However, the Hellenic state has failed to argue why such a processing activity will be strictly necessary, and has not provided for any type of related appropriate safeguards. None of the conditions provided for in Article 10 are met, since there is no related Union or Greek law in place, the processing does not protect the vital interests of data subjects, nor does it relate to data that is manifestly made public by the data subjects. Thus, there are strong indications that the Hellenic Police do not have any available lawful basis for the envisaged data processing activity (E. Chelioudakis, 2020).[15]

6. Conclusion

The exploration of Law 4624/2019 (GDPA) reveals significant discrepancies and potential challenges with regard to the implementation of the LED. Whether discussing the processing of special categories of data, the limitations to a data subject's rights, or the conditions under which access to information is granted, it is evident that the Greek legislation often introduces broader, vaguer criteria that may undermine the strict

[15] Insufficient information is available at the time of drafting the report for another project called REACTION. This appears to be a research project co-funded by Greece, Cyprus, and the EU Integrated Border Management Fund. It aims to develop a next-generation platform for border surveillance that can provide situational awareness at remote frontier locations as an efficient tool for a rapid response to critical situations. Alexandra Karaiskou, Drones & Artificial Intelligence at Greece's high-tech borders, 2023

protections intended by the EU law's framework. At the same time, the Greek state has adopted a number of different technology-led applications in the field of law enforcement, while the Hellenic DPA, seriously understaffed, struggles to cope with related investigations.

7. Policy Recommendations

The following policy recommendations aim to address the significant gaps and weaknesses in Greece's current legal framework concerning the transposition of the LED. These recommendations are designed to strengthen data protection safeguards, enhance accountability in law enforcement data processing, and ensure that the Greek framework better aligns with the LED's requirements, safeguarding the rights and freedoms of individuals.

- **Article 49 GDPA:** This article should not make references to "consent" as a legal basis for processing personal data by law enforcement authorities. According to Recital 35 of the LED, consent cannot be considered valid in these contexts because individuals cannot freely refuse, given the imbalance of power in law enforcement scenarios. This change will prevent any misuse of consent in coercive or unequal situations. The references to the term "consent" should be replaced with references to the term "voluntary agreement", in line with Recital 35 LED and the guidance provided by Article 29 Working Party (WP29). "Voluntary agreement" is not a legal basis: as the text of Recital 35 LED underlines, Member States may provide by law that the data subject may agree to the processing of his or her own personal data for the purposes of Directive 2016/680, such as DNA testing in criminal investigations or the surveillance of his or her location with electronic tags, for the purpose of executing criminal sanctions.

- **Article 54 GDPA:** This article introduces broader justifications for delaying or withholding information from data subjects compared to the LED. Specifically, the GDPA uses the term "enabling" competent authorities to perform their duties, which expands the scope for withholding information beyond the more restrictive conditions outlined in the LED. Additionally, it replaces "rights and freedoms of others" with the broader and more ambiguous term "legitimate interests of third parties", potentially weakening protections for data subjects. Article 54 GDPA should be revised to align more closely with the LED by narrowing the scope for withholding information.

- **Article 56 GDPA:** This article introduces two additional grounds for denying a data subject's right to erasure that are not in line with Article 16 of the LED. Specifically, these include: (1) retaining data if erasure would compromise the legitimate interests of the data subject, and (2) retaining data if erasure would involve disproportionate effort due to "special storage modes". These provisions undermine the data subject's rights and risk misuse by law enforcement agencies or data controllers. Additionally, Article 56 GDPA fails to transpose an essential ground from Article 16 LED regarding situations where the accuracy of personal data is contested by the data subject. The provision allowing law enforcement agencies or data controllers to retain personal data based on the assumption that erasure would compromise the data subject's legitimate interests should be removed. This provision is overly paternalistic and undermines the autonomy of individuals to control their personal data. Instead, the focus should be on the data subject's right to decide whether their data should be erased, without allowing controllers to

override that decision based on their interpretation of the subject's interests. Moreover, the vague and broad exception for retaining data due to "special storage modes" should be removed, too. This clause could be misused to retain data indefinitely, circumventing the right to erasure. Data controllers should be required to implement technical and organisational measures that ensure data can be erased when required, rather than using storage complexity as an excuse for non-compliance. Lastly, the GDPA should introduce the missing provision from Article 16 LED, which allows for restricting processing rather than erasure when the accuracy of the personal data is contested by the data subject and the accuracy or inaccuracy cannot be ascertained. This would provide a balanced approach, ensuring that data is not erased prematurely while disputes about its accuracy are resolved.

8. Glossary of Laws cited in this report

-Greek Law 4624/2019, also known as The Greek Data Protection Act (GDPA): Its latest version (2022 onwards) is available in the original Greek: https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019. The only English translation provided by the Hellenic Data Protection Authority does not take into consideration the revisions of 2022. It is available at the following link: https://www.dpa.gr/sites/default/files/2020-08/LAW 4624_2019_EN_TRANSLATED BY THE HDPA.PDF.. Wherever possible, this translation was used for references here. When references were needed for the revised parts of Law 4624/2019, an unofficial translation by the author was provided.

-Greek Law 5002/2022: This Law included provisions revising Law 4624/2019 with regard to the transposition of the LED, among other topics. There is no official translation of the Law in English, but the Greek version is available at: https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022.

-**Presidential Decree 75/2020:** This PD provided for the use of cameras by LEAs in public spaces. There is no official translation of the PD in English, but the Greek version is available at: https://www.kodiko.gr/nomothesia/document/638933/p.d.-75-2020.

9. Bibliography

Article 29 Working Party on Data Protection, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) - WP258, 2017, https://ec.europa.eu/newsroom/article29/items/610178/en

Chelioudakis, E, "Greece: Technology-led policing awakens", 2020, https://aboutintel.eu/greece-policing-border-surveillance/

Chelioudakis, E, "Unpacking AI-enabled border management technologies in Greece: To what extent their development and deployment are transparent and respect data protection rules?", 2024, Computer Law & Security Review, Elsevier, https://www.sciencedirect.com/science/article/abs/pii/S0267364924000347

European Commission, Infringement Case INFR(2018)0157 against Greece, 2018.

European Commission, Data protection: Commission decides to refer Greece and Spain to the Court for not transposing EU law, July 2019, https://ec.europa.eu/commission/presscorner/detail/EN/IP_19_4261

European Digital Rights, "Facial recognition: Homo Digitalis calls on Greek DPA to speak up", 2020, https://edri.org/our-work/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/

Hellenic Data Protection Authority (2020a), Γνωμοδότηση 1/2020 επί των διατάξεων του Ν. 4624/2019, January 2020, https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epi-ton-diataxeon-toy-n-46242019

Hellenic Data Protection Authority (2020b), Request for Information with regard to the smart-policing contract between the Hellenic Police and Intracom-Telecom (EL), 2020, https://www.homodigitalis.gr/wp-content/uploads/2020/09/ΑΠΔΠΧ_SmartPolicingContract_31.08.2020.pdf

Hellenic Data Protection Authority, Γνωμοδότηση 5/2022 επί του σχεδίου νόμου "Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών", November 2022, https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gnomodotisi-epi-toy-shedioy-nomoy-diadikasia-arsis-toy-aporritoy-ton

Hellenic Data Protection Authority (2022b), Follow-up request before the Hellenic Police regarding the smart policing project, 2022, https://www.homodigitalis.gr/wp-content/uploads/2022/10/HDPA_SmartPolicing_2022.pdf

Hellenic Data Protection Authority 2022-2024, e-newsletter. The HDPA has been publishing related reports periodically, every three months, more precisely:

- from 19/1/2024 to 23/4/2024 https://www.dpa.gr/sites/default/files/2024-04/April2024.pdf ,
- from 20/10/2023 to 18/1/2024 https://www.dpa.gr/sites/default/files/2024-01/Jan2024.pdf,
- from 11/7/2023 to 19/10/2023 https://www.dpa.gr/sites/default/files/2023-10/Oct2023.pdf,
- from 7/4/2023 to 10/7/2023 https://www.dpa.gr/sites/default/files/2023-07/July2023.pdf,
- from 17/1/2023 to 6/4/2023 https://www.dpa.gr/sites/default/files/2023-04/April2023.pdf,
- from 16/10/2022 to 16/01/2023 https://www.dpa.gr/sites/default/files/2023-01/Jan2023.pdf,
- from 15/7/2022 to 15/10/2022 https://www.dpa.gr/sites/default/files/2022-10/Oct2022.pdf,
- from 16/4/2022 to 14/7/2022 https://www.dpa.gr/sites/default/files/2022-07/July2022.pdf,
- from 15/1/2022 to 15/4/2022 https://www.dpa.gr/sites/default/files/2022-04/April2022.pdf,
- from 14/10/2021 to 14/1/2022 https://www.dpa.gr/sites/default/files/2022-01/Jan2022.pdf,
- from 22/4/2021 to 12/7/2021 https://www.dpa.gr/sites/default/files/2021-07/July2021_0.pdf,
- from 9/2/2021 to 21/4/2021 https://www.dpa.gr/sites/default/files/2021-04/April2021_0.pdf, and
- from 6/10/2020 to 8/2/2021 https://www.dpa.gr/sites/default/files/2021-02/Feb2021_0.pdf .

Hellenic Police, The technical specifications of the smart policing contract, 2018, https://www.astynomia.gr/images/stories/2018/prokirikseis18/12042018-texn_prod.pdf

Hellenic Police, Response to Submission of questions and requests for access to documents and information regarding the use of drones and the use of body cameras in the equipment of police officers by the Hellenic Police, March 2021, https://homodigitalis.gr/wp-content/uploads/2021/05/HellenicPolice_Reply.pdf

Hellenic Police, Statistical Data, Accessed in August 2024, https://www.astynomia.gr/statistika-stoicheia/

Hellenic Republic, Acceptance of Financial Offer, 2022, https://diavgeia.gov.gr/doc/97244653ΠΩ-ΞΟ1?inline=true

Homo Digitalis (2019a), "Complaint lodged by Homo Digitalis against Greece for non-compliance with the EU's data privacy law addressed to the European Commission", May 2019, https://homodigitalis.gr/en/posts/3988/

Homo Digitalis (2019b), "Σχόλια επί του Σχεδίου Νόμου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα", August 2019, https://homodigitalis.gr/wp-content/uploads/2019/08/σχόλια_Σχέδιο-Νόμου-για-την-Προστασία-Δεδομένων-Προσωπικού-Χαρακτήρα_HD-1.pdf

Homo Digitalis (2019c), "Complaint submission to the European Commission regarding Law 4624/2019", October 2019, https://homodigitalis.gr/en/posts/4603/

Homo Digitalis (2019d), "Hellenic Police plans to introduce face recognition technology", 2019, https://www.homodigitalis.gr/en/posts/4965

Homo Digitalis (2020a), "Homo Digitalis complaint to the European Commission: An update", June 2020, https://homodigitalis.gr/en/posts/7035/

Homo Digitalis (2020b), "Insufficient response of the Hellenic Police for the contract for the development of facial recognition software", 2020, https://www.homodigitalis.gr/posts/5125

Homo Digitalis & EKPIZO (2019), "Official Request to the Hellenic Data Protection Authority for the issuance of legal opinion on Law 4624/2019", September 2019, https://homodigitalis.gr/en/posts/4217/.

Homo Digitalis (2021), "Notification of an infringement of the provisions of P.D. 75/2020 from the Hellenic Police, and Request to the DPA to exercise its powers", May 2021, https://homodigitalis.gr/wp-content/uploads/2021/05/Γνωστοποίηση-Παράβασης-των-διατάξεων-του-ΠΔ752020-και-αίτημα-άσκησης-των-σχετικών-εξουσιών.pdf

Homo Digitalis (2022), "The Hellenic Coast Guard wants to acquire social media monitoring software: The Hellenic DPA is urged to exercise its investigative and supervisory powers", 2022, https://www.homodigitalis.gr/en/posts/10848

Homo Digitalis, "The Hellenic DPA is investigating the Greek Coast Guard for social media monitoring", 2023, https://www.homodigitalis.gr/en/posts/12490

Human Rights Watch, "Greek Police Abuses of Migrants in Athens", 2013, https://www.hrw.org/report/2013/06/12/unwelcome-guests/greek-police-abuses-migrants-athens

Human Rights Watch & Homo Digitalis, "Greece: New Biometrics Policing Program Undermines Rights", 2022, https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

Karaiskou, A., "Drones and Artificial Intelligence at Greece's high-tech borders", 2023, https://homodigitalis.gr/en/posts/131019/.

Ministry of Citizen Protection, Payment Order on Smart Policing project, 2021, https://diavgeia.gov.gr/doc/6ΦΚΞ46ΜΤΛΒ-ΖΒΚ?inline=true

Ministry of Shipping and Island Policy of the Hellenic Republic, Open Call for the upgrade/maintenance of the computer room of the Directorate of Maritime Border Security and Protection, 2022, https://diavgeia.gov.gr/doc/ΨΒΥΤ4653ΠΩ-ΑΘΒ

Zafeiropoulos, K. "The DPA is investigating the Coast Guard for social media monitoring", 2023, https://www.efsyn.gr/ellada/koinonia/389257_i-arhi-prostasias-prosopikon-dedomenon-ereyna-limeniko-soma-gia

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights