GALA

GLOBAL ADVERTISING LAWYERS ALLIANCE

THIRD EDITION

Privacy Law: A Global Legal Perspective

on Data Protection Relating to Advertising and Marketing

Privacy Law: A Global Legal Perspective on Data Protection Relating to Advertising and Marketing

THIRD EDITION

This publication provides general guidance only. It does not provide legal advice.
Please consult your attorney for legal advice.

©2025 Global Advertising Lawyers Alliance

FOREWORD

Since the last edition of this book in 2022, the legal and technological landscape for advertising and marketing has shifted dramatically. The rapid adoption of artificial intelligence, the tightening control of platforms and browsers on data flows, and a surge of new and strengthened privacy laws around the world have reshaped how brands, agencies, publishers, and platforms understand and connect with consumers. Data remains the lifeblood of the advertising ecosystem, powering research and analytics, attribution and measurement, personalized marketing, and entirely new ways to reach audiences, but the rules governing that data are evolving at unprecedented speed.

The past three years have seen privacy and data protection move even further from a compliance obligation to a strategic business priority. Dozens of jurisdictions have enacted or strengthened comprehensive privacy frameworks, many modeled on the GDPR but increasingly going beyond it with stricter consent standards for targeted advertising, broader definitions of personal data, and AI-specific obligations. In the United States alone, the number of state privacy laws has more than doubled, adding expanded rights for sensitive data, enhanced opt-out mechanisms for targeted advertising, and heightened enforcement. Countries across Asia, Africa, and Latin America have followed suit, many introducing stringent cross-border transfer restrictions and data localization mandates that complicate global campaigns.

At the same time, enforcement activity has accelerated. Regulators are issuing record fines for unlawful profiling, noncompliance with transparency and consent obligations, and violations of children's privacy. Privacy enforcement is also converging with competition and consumer protection law, changing how authorities assess the fairness of data-driven advertising practices. For advertisers, this means compliance now requires a more holistic view of legal risk, spanning privacy, market competition, and consumer trust.

And then there's AI. Generative AI and predictive analytics tools are now embedded in advertising workflows, from creative generation to media buying, raising fresh questions about lawful data sourcing, fairness, bias mitigation, and accountability. Regulators are

signaling that existing privacy and marketing rules apply with full force to these tools, and in some jurisdictions, AI-specific obligations aimed at ensuring transparency, human oversight, and ethical use have been layered on top.

This third edition of Privacy Law and Data Protection: A Global Legal Perspective on Advertising and Marketing, produced by the Global Advertising Lawyers Alliance (GALA), remains unmatched in scope and focus: a comprehensive, jurisdiction-by-jurisdiction guide to privacy and data protection laws in the advertising and marketing sector, written by leading local experts in 78 countries. Each chapter provides the legal framework, practical implications for advertisers, and insights into where the law is heading.

On behalf of GALA, I am grateful to every contributor for the time, expertise, and clarity they brought to this work. In a world where laws, technology, and public expectations continue to evolve at a rapid pace, we hope this 2025 edition serves as an essential, authoritative resource for navigating the complex intersection of privacy, data protection, and advertising law.

Daniel Goldberg
Frankfurt Kurnit Klein & Selz, PC

September 2025

ABOUT GALA

The Global Advertising Lawyers Alliance (GALA) is the leading network of advertising lawyers in the world. With firms representing more than 90 countries, each member has the local expertise and experience in advertising, marketing and promotion law that will help your campaign achieve its objectives, and navigate the legal minefield successfully. GALA is a uniquely sensitive global resource whose members maintain frequent contact with each other to maximize the effectiveness of their collaborative efforts for their shared clients. GALA provides the premier worldwide resource to advertisers and agencies seeking solutions to problems involving the complex legal issues affecting today's marketplace.

For further information about GALA, please contact the relevant member directly or alternatively GALA's Executive Director, Stacy Bess at:

Global Advertising Lawyers Alliance
28 Liberty Street, 35th Floor, New York, NY 10005
Tel: 212.705.4895 | Fax: 347.438.2185
Email: sbess@galalaw.com
www.galalaw.com

GREECE

1 PRIVACY LAW

1.1 Provide a brief summary of how privacy is regulated in Greece.

Privacy in Greece is, first of all, protected at a constitutional level, by the Greek Constitution, which provides that: 'All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law.'

Furthermore, the protection of personal data is specifically regulated in Greece; primarily, by European Law and, complementarily, by national law.

More specifically, as in all EU Member States, the primary source of privacy law in Greece is the General Data Protection Regulation 2016/679 ('GDPR') (see the European Union chapter).

Additionally, national Law No 4624/2019 ('Greek Data Protection Law') sets some rules regarding the implementation of certain aspects of the GDPR in Greece, in relation to which the GDPR contains opening clauses. These national rules either specify or limit some of the rights and obligations provided by the GDPR.

Privacy rules in the electronic communications sector are also set by Greek Law No 3471/2006 (as amended), which implemented the ePrivacy Directive.

1.2 What are the primary laws regulating privacy in Greece? Include national, state, local, and sector-specific laws, with an emphasis on those impacting advertising.

Privacy in Greece is mainly regulated by the GDPR, which came into force, as in all Member States, on May 25, 2018 and is directly applicable in Greece, with no need of incorporation by the national legislator (see the European Union chapter).

Additionally, the Greek Data Protection Law, which entered into force on August 29, 2019, sets specific provisions regarding the implementation of certain aspects of the GDPR in Greece, and also incorporates the EU Law Enforcement Directive (2016/680) into Greek law.

The most important provisions relating to private entities in the Greek Data Protection Law, which are supplemental to the provisions of the GDPR, concern:

(a) consent of minors to processing of their personal data in relation to information society services (see question 3.2);
(b) processing of special categories of personal data for certain purposes other than those provided in the GDPR (see question 3.2);
(c) prohibition on processing of genetic data for purposes of health and life insurance (see question 3.2);
(d) processing of personal data for further purposes other than those for which the data had been collected;
(e) processing of personal data in the context of employment;
(f) processing of personal data in specific situations, such as academic, artistic or literary expression and journalistic purposes, scientific or historical research purposes, or for the collection or retention of statistics;

(g) exceptions from the obligation to inform data subjects; exceptions to the right of access and to the right of erasure; and release from the obligation to communicate a data breach to the data subject in specific cases ; and

(h) penal sanctions for specific willful violations of data protection law.

The Greek Data Protection Law has also repealed Greek Law No 2472/1997 (which had been the main legislative text regulating protection of personal data in Greece prior to the GDPR), with the exception, however, of certain specific provisions which still remain in force, such as the right of data subjects to declare to the Hellenic Data Protection Authority that they do not want their personal data to be processed by anybody for purposes of marketing communication by post.

In addition, especially in relation to the protection of privacy in the electronic communications sector, Greek Law No 3471/2006 provides rules for marketing communications by electronic means.

1.3 What role does self-regulation play in privacy regulation, particularly for advertising practices?

Advertising self-regulation has gained much importance in Greece in recent years. The main self-regulation organization in Greece is the Advertising Self-Regulation Council ('SEE') which is a member of the European Advertising Standards Alliance ('EASA') and enforces the Hellenic Code of Advertising and Communication Practice ('HCACP').

The structure and content of the HCACP is almost identical to the ICC Consolidated Code of Advertising and Communication Practice. The HCACP covers both non-broadcast and broadcast advertising, including online advertising and social media. The HCACP sets forth specific provisions on the protection of personal data and privacy. The HCACP also has a special Chapter on direct marketing and digital marketing communications, which includes privacy-related provisions.

SEE may be activated either after an ex officio monitoring or after submission of a written complaint. Both consumers and competitors are entitled to file complaints claiming that a marketing communication breaches the HCACP.

However, as noted in the European Union chapter, self-regulation is only a supplementary mechanism in relation to enforcing privacy rules. The main authority responsible for monitoring compliance with privacy law in Greece is the Hellenic Data Protection Authority ('Hellenic DPA'), which is an independent supervisory authority (see question 1.4).

1.4 How is privacy law enforced in Greece? Discuss the roles of regulators, self-regulatory bodies, private actions, and other enforcement mechanisms.

The independent supervisory authority responsible for monitoring the implementation and enforcement of privacy law in Greece is the Hellenic DPA. The Hellenic DPA has the competency, inter alia, to handle complaints, investigate possible breaches of privacy law, issue decisions and impose administrative sanctions (including monetary fines) in cases of violation of data protection rules.

In addition, data subjects who wish to seek compensation or other form of restitution in cases of unlawful processing of their personal data by a controller or processor, may bring civil actions before the competent civil courts, which will, in this case, also enforce privacy law.

Furthermore, in cases of penal violations in relation to personal data, which are specifically provided in the Greek Data Protection Law, the penal courts are also competent to enforce the data protection rules.

2 APPLICABILITY

2.1 What makes a company subject to privacy law in Greece?

As far as the GDPR is concerned, please see the European Union chapter.

The Greek Data Protection Law applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, by public or private bodies, with the exception of processing of personal data by a natural person in the course of a purely personal or household activity. 'Private bodies' are considered to be all natural or legal persons or associations of persons without legal personality, that do not fall within the definition of 'public bodies'. Thus, as is the case with the GDPR, all companies fall under the obligations of the Greek Data Protection Law, subject only to its territorial scope (see question 2.2).

2.2 Does privacy law in Greece apply to foreign companies? If so, under what conditions? Are there specific requirements for foreign companies (eg, appointing a local representative)?

Yes, Greek privacy law can apply to companies outside Greece.

As far as the GDPR is concerned, please see the European Union chapter.

The Greek Data Protection Law applies to private bodies when:

(a) a controller or processor processes personal data in Greece, or

(b) personal data is processed in the context of the activities of an establishment of a controller or a processor in Greece, or

(c) even if the controller or the processor does not have an establishment in the EU/EEA, they fall within the scope of the GDPR.

In cases where a controller or processor, who falls under the scope of the law, is established outside the EU, they should designate a representative in writing (please see the European Union chapter).

3 PERSONAL DATA

3.1 How is personal data defined under privacy law in Greece?

The GDPR definition applies (see the European Union chapter). There is no different definition of 'personal data' in the Greek Data Protection Law.

3.2 What categories of personal data are considered sensitive, and how are they regulated differently?

See the European Union chapter.

Also, in relation to the 'special categories of personal data', the Greek Data Protection Law exceptionally permits private bodies to process such categories of personal data, if the processing is necessary:

(a) to exercise rights derived from the right of social security and social protection and to meet the related obligations; or

(b) for the purposes of preventive medicine, for the assessment of the working capacity of the employee, for medical diagnosis, for the provision of health or social care or treatment or for the management of health or social care systems and services, or pursuant to the data subject's contract with a health professional or other person who is subject to the obligation of professional secrecy or is under their supervision.

In the above cases, of course, appropriate and specific measures need to be taken to safeguard the interests of the data subject.

In addition, processing of genetic data for purposes of health and life insurance is prohibited.

With regards to personal data of children, the Greek Data Protection Law provides that, when consent is the legal basis for processing of non-sensitive personal data of children in relation to information society services, a child should be at least 15 years old in order to give valid consent. If the minor is below the age of 15, the consent of the person holding parental responsibility is required.

3.3 How are anonymized, pseudonymized, or de-identified data treated under privacy law?

See the European Union chapter.

4 COMPANY OBLIGATIONS

4.1 What are the key obligations for companies under privacy law (eg, transparency, consumer rights, data minimization, contracts, record-keeping, training)?

See the European Union chapter.

4.2 Are companies assigned roles based on their processing activities (eg, controller versus processor)? How do these roles affect their obligations?

See the European Union chapter.

4.3 Does privacy law require a lawful basis for processing personal data (eg, legitimate interest, consent)? If so, explain.

See the European Union chapter.

5 TRANSPARENCY AND CONSUMER RIGHTS

5.1 What information must companies include in their privacy notices when processing personal data for advertising purposes?

See the European Union chapter.

5.2 What privacy rights do consumers have concerning their personal data in advertising contexts?

See the European Union chapter. Also, see question 1.2 in relation to limitations of data subjects' rights provided by the Greek Data Protection Law.

5.3 Under what circumstances must companies obtain consent or provide opt-out options for advertising activities? What measures are required?

See the European Union chapter.

6 CONTRACTS AND DUE DILIGENCE

6.1 How does privacy law address the use of vendors and other third parties in advertising (eg, advertising agencies, DSPs, SSPs, or data providers)?

See the European Union chapter.

6.2 What contractual obligations must companies fulfil when disclosing or receiving personal data to or from vendors or other third parties?

See the European Union chapter.

6.3 What due diligence measures are companies expected to undertake in their privacy practices? When are impact assessments required for advertising uses?

See the European Union chapter.

Also, the Hellenic DPA has issued a list of processing activities for which it considers that it is obligatory to carry out a data protection impact assessment ('DPIA'). The list, inter alia, includes cases of systematic data processing for marketing purposes which involve profiling of natural persons, when the data are combined with data collected from third parties.

7 SPECIFIC ADVERTISING PRACTICES

7.1 How is direct marketing (eg, emails, texts, push notifications) regulated under privacy law?

See the European Union chapter for privacy law obligations.

In addition:

(a) With regard to marketing communications through electronic means, such as by email, SMS, fax, automated calls, etc (with the exception of calls made with human intervention), it is necessary, as a general rule, that the receiver of the communication/data subject has provided valid, informed and explicit consent prior to the communication ('opt-in' system). In a decision in 2022, the Hellenic DPA deemed that the same requirements also apply when sending marketing communications to an email address belonging to a legal entity.

Nevertheless, in cases where the electronic contact details have been previously acquired legally in the framework of a commercial relationship with the data subject (eg, previous sale of products or provision of services to the data subject), it is possible to use such data for future marketing communication in relation to similar products or services, even if the recipient of the communication had not provided prior explicit consent (it is noted that in a decision in 2022, the Hellenic DPA ruled that being 'connected' with the data subject on LinkedIn does not suffice in order to add the data subject's email to a newsletter recipient list without consent). However, it is absolutely necessary to provide, both when the data is collected as well as in each communication, a clear, easy and free way for data subjects to

object to the collection and use of their contact details in the future ('soft opt-in' system). In a decision in 2019, the Hellenic DPA imposed a fine of €200,000 on a leading Greek telecommunications provider, because it was found that, starting from 2013, about 8,000 recipients of advertising emails were not able to successfully use the 'unsubscribe link' provided in the emails in order to object to receiving the provider's further marketing communications, due to a technical error that had not previously been detected. This situation was deemed by the Hellenic DPA to be in violation of the right of data subjects to object to processing for direct marketing purposes, as well as to the principle of privacy by design, provided by the GDPR.

(b) Regarding phone calls made with human intervention for direct marketing purposes, consumers have the right to declare, for free, to their telecommunication provider that they do not wish to receive this kind of marketing calls ('opt out' system). Each telecommunication provider has the obligation to keep a registry of the subscribers who have provided this declaration; and any interested party who wishes to make direct marketing calls should previously check the registries kept by each provider and comply with them. In relation to this matter, the Hellenic DPA in 2019 imposed a considerable administrative fine of €200,000 on a leading Greek telecommunications provider for not keeping the registry provided to advertisers properly updated. This resulted in phone calls to subscribers who had opted out of this kind of direct marketing. The incident was found by the Hellenic DPA to infringe the principle of accuracy and to the principle of data protection by design, provided by the GDPR.

(c) The Hellenic DPA also keeps a registry of data subjects who do not wish to receive marketing communications by traditional post. It is a legal obligation for data controllers to check this opt-out registry prior to sending such marketing communications.

(d) In relation to marketing communications through the Viber app, in 2018, the Hellenic DPA issued a decision which provides some guidance to private companies (data controllers). According to this decision, the lawfulness of sending Viber messages for direct marketing purposes can be based either on the consent of the data subject or on the legitimate interests of the data controller. In addition, the Hellenic DPA considered that accepting to receive such messages from the data controller through the 'Viber business' service did not constitute valid consent, since it did not meet the criteria in the Greek privacy law in force at the time, nor the GDPR. This is because the data subject was not properly informed of the purpose of the processing (namely the promotion of products/services of the company) during the collection of the data; nor was the purpose of sending the message adequately defined at the point of sending.

7.2 How are tracking technologies (eg, cookies, pixels, SDKs) regulated under privacy law?

See the European Union chapter.

7.3 How are loyalty programs and promotions regulated under privacy law?

See the European Union chapter.

7.4 How is social media and influencer marketing regulated under privacy law?

See the European Union chapter.

7.5 How does privacy law regulate targeted advertising (including behavioral or personalized advertising), and how does the law differ in its treatment of contextual advertising?

See the European Union chapter.

7.6 How are digital identity resolution and clean room technologies regulated under privacy law?

See the European Union chapter.

7.7 How is location-based advertising regulated under privacy law?

See the European Union chapter.

7.8 How are data brokers defined and regulated under privacy law?

See the European Union chapter.

7.9 How is advertising to children and minors regulated under privacy law?

The Greek Data Protection Law provides that, when consent is the legal basis for the processing of non-sensitive personal data of children in relation to information society services, a child should be at least 15 years old in order to give valid consent. If the minor is below the age of 15, the consent of the person holding parental responsibility is required.

See also the European Union chapter.

7.10 How does privacy law regulate profiling or the use of artificial intelligence or automated decision-making technology for advertising purposes?

See the European Union chapter.

7.11 Are there other specific advertising practices that you wish to discuss?

See question 11.2 in relation to 'dark patterns'.

8 DATA TRANSFERS

8.1 Are there restrictions on transferring personal data across jurisdictions? What safeguards or mechanisms are required for such transfers (eg, standard contractual clauses)? Are there specific countries or jurisdictions where certain transfers are prohibited?

See the European Union chapter.

8.2 Are there any additional considerations for personal data transfers (eg, privilege concerns)?

See the European Union chapter.

9 DATA SECURITY AND BREACH MANAGEMENT

9.1 How is data security regulated in Greece? Are there minimum standards? Does this differ by sector or size of the entity?

See the European Union chapter.

9.2 How are personal data breaches regulated in Greece? What are the requirements for notification and response?

See the European Union chapter.

10 ENFORCEMENT AND PENALTIES

10.1 What penalties exist for non-compliance with privacy law?

See the European Union chapter regarding the administrative sanctions.

In addition, the Greek Data Protection Law provides also penal sanctions for specific willful violations of data protection law.

10.2 Do consumers have a private right of action? What remedies are available to them?

See the European Union chapter. See also our answer to question 1.4 above.

10.3 How active are enforcers in privacy-related matters? Provide examples of enforcement actions or lawsuits for alleged privacy non-compliance involving advertising.

In recent years, the Hellenic DPA has handled a number of cases that involve advertising, especially regarding issues of direct marketing by email, SMS or phone calls. The sanctions issued, if GDPR violations are found, are determined on a case-by-case basis. See, for example, question 7.1, in relation to two considerable administrative fines, each amounting to €200,000, that were imposed on a leading telecommunications provider in Greece in relation to issues of direct marketing.

11 EMERGING CONSIDERATIONS

11.1 Are there cultural considerations that impact privacy law or enforcement in Greece?

No.

11.2 What are the 'hot topics' or anticipated legal challenges that companies should monitor?

The prohibition on 'dark patterns' is a topic that companies should be aware of, especially in relation to online marketing and online tracking methods. Depending on the case, dark patterns may violate various legal provisions, and especially consumer protection and data protection laws.

In relation to privacy, dark patterns may particularly infringe the rules for legitimately obtaining a person's informed consent, as well as the legal principles of transparency, privacy-by-design and privacy-by-default. In this context, the European Data Protection Board has also adopted Guidelines on 'deceptive design patterns in social media platform interfaces'.

It is also noted that, for cases not covered by legislation on consumer protection or data protection, the EU Digital Services Act ('DSA') expressly sets a 'ban' on dark patterns in online platforms, by prohibiting the platforms from designing, organizing or operating their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs a user's ability to make free and informed choices. In addition to the DSA, the Digital Markets Act ('DMA'), the Data Act and the AI Act also contain provisions that prohibit specific dark patterns.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or insights?

The Hellenic DPA has issued rather heavy administrative fines to companies in cases of major violations of the GDPR. For example:

(a) In July 2022, the Hellenic DPA imposed a fine of €20 million on a very well-known American facial recognition company for various GDPR violations, and ordered it to not collect and process personal data of data subjects located in Greece by using facial recognition technology, and to delete any data already collected.

(b) Regarding data breaches, in January 2022, the Hellenic DPA imposed very heavy fines of €9.25 million in total on a major Greek mobile operator and its parent company, a major telecommunications provider, for various GDPR violations related to the circumstances of a cyberattack that took place in 2020, which affected millions of data subjects.

(c) Another considerable fine of almost €3 million was imposed in February 2024 on a leading postal service provider in Greece, following a cyberattack which resulted in the leakage of personal data on the dark web, because the Hellenic DPA deemed that the data controller had failed to implement appropriate technical security measures and to effectively apply policies regarding the protection of personal data.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have occurred since this book was last published in 2022? What triggered these changes?

See the European Union chapter.

12.2 What are the biggest challenges companies face due to the changing privacy landscape?

See the European Union chapter.

12.3 What do you envision the privacy landscape will look like in five years?

The decisions and guidelines that the Hellenic DPA issues over the years have a great importance for the interpretation and application of the GDPR in Greece; therefore, companies need to seek local legal advice in case Greek privacy rules apply.