onetrust
DataGuidance

EU: Processing telecoms data under the ePrivacy Directive

BAHAS, GRAMATIDIS
& PARTNERS LLP

The ePrivacy Directive regulates personal data processing in electronic communications, complementing the GDPR with national variations.

Directive 2002/58/EC (the ePrivacy Directive) governs the processing of personal data and the protection of privacy in the electronic communications sector. It addresses sector-specific issues such as traffic data, location data, and confidentiality of communications, complementing the General Data Protection Regulation (GDPR).

In this Insight article, Popi Papantoniou and Konstantinos Psevdos, of Bahas, Gramatidis & Partners, explore the legal requirements for processing traffic data as well as the exceptions to these conditions, particularly where fraud prevention is concerned. Due to the nature of the ePrivacy Directive, divergences occur in the process of national implementation across the EU Member States and shall be examined along with key case law from EU courts and national regulators.

Overview of the ePrivacy Directive and its scope

The ePrivacy Directive is binding upon Member States and implemented into national law. Article 2 of the ePrivacy Directive presents the definitions of key terms, which are necessary for a better understanding of its scope. In this regard, traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof, while location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

Most importantly, the term communication includes any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This, however, does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

According to Article 3 of the ePrivacy Directive, the scope of its application covers the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the community.

This restriction led to much debate, since the distinction between private and public networks and services can be difficult.1 Communication data includes traffic and location data. It is clear that the ePrivacy Directive operates alongside the GDPR. However, it functions as a lex specialis - meaning in the case of both laws applying to the same subject, the ePrivacy Directive takes precedence. In cases of processing of personal data not covered by the ePrivacy Directive, the GDPR applies residually.

Cookie Law

Also named the 'Cookie Law,' the ePrivacy Directive, as amended in 2009, regulates, among others, the use of cookies on websites. Cookies are small text files stored on a user's device when they visit a website. Under Article 5(3) of the ePrivacy Directive, user consent is required before the operation of cookies on a certain website. However, cookies solely necessary to provide an information society service explicitly requested by the subscriber or user are an exception to the rule of prior consent. Consent should be given in the context of the GDPR and the former Data Protection Directive 95/46/EU. Interpreted by the Court of Justice of the European Union (CJEU), this means that the information regarding consent should be clear and comprehensive and include the duration of the operation of cookies, the different types of cookies, and whether or not third parties may have access to those cookies.2 In cases where the cookies regard sensitive personal data, consent must be explicit. Furthermore, Article 5(3) of the ePrivacy Directive does not differentiate between types of data stored or accessed. The term 'information' is broader than personal data, thus the protection from cookies by the ePrivacy Directive is broader and subject to the protection of the GDPR. With Guidelines 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive, the European Data Protection Board (EDPB) extended the application of the ePrivacy Directive to several modern tracking technologies.

General requirements for processing traffic data

Under Article 6 of the ePrivacy Directive, traffic data (as defined above), which relates to subscribers and users, processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. This general rule is followed by certain exceptions where processing is permitted in cases of:

- billing and interconnection payments, where providers may solely process data necessary for subscriber billing or settlement of payments and only up to the end of the period during which the bill may lawfully be challenged or payment pursued; or
- user consent for marketing of electronic communications services (opt-in) or provision of value-added services, to the extent and for the duration necessary for such services or marketing, with the option for the user to withdraw their consent at any time.

The data subject must be duly notified by the service provider conducting the processing as to the types of traffic data processed and the duration of such processing. Where user consent is required, the relevant notice should be provided prior to its collection. In any case, the data collected should be limited in scope and its processing restricted to persons involved in network management, billing, complaints handling, marketing, or fraud detection.

Location data other than traffic data

Article 9 of the ePrivacy Directive specifically regulates the processing of location data other than traffic data as detailed above. This type of data includes information revealing the geographic position of a user, i.e., GPS data, cell ID, Wi-Fi access point location, and Bluetooth.3 Such data may be processed when made anonymous or with the consent of the data subject. The requirements above for the processing of traffic data apply accordingly, meaning that in the case of consent, the user should be informed prior to its collection, while maintaining the option of withdrawing it at any time. In any case, the processing should reach the extent and the duration necessary for the provision of a value-added service.

In correlation to the traffic data above, location data may be processed solely by persons under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value-added service.

Processing data for fraud prevention purposes

Fraud prevention is not explicitly listed as grounds for processing traffic or location data under the ePrivacy Directive. The duty of security burdening public service providers under the Directive could present as grounds for limited data processing by the said providers. Article 4 of the ePrivacy Directive, which obliges service providers to 'take appropriate technical and organizational measures to safeguard the security of their service,' could be interpreted as the above duty of security. This may allow for basic fraud detection and mitigation activities, not beyond what is strictly necessary for ensuring security, while not overriding the above erasure requirement of Article 6 of the ePrivacy Directive.

While the GDPR, particularly Article 6, as interpreted by the EDPB, entails fraud prevention in the meaning of 'legitimate interest' for data processing, the ePrivacy Directive takes precedence over the GDPR regarding communications data (as also emphasized by the EDPB). In any case, where fraud prevention activities include the processing of traffic data as detailed in the ePrivacy Directive, this processing may be conducted on the basis of the duty of security of public service providers if interpreted as such.

Unsolicited communications

Article 13 of the ePrivacy Directive adopts a general opt-in system, which demands users' prior consent for the use of cookies (see above) and direct marketing communications (i.e., promotional emails, SMS, and automated calls). An exception to the general opt-in rule constitutes marketing communication to existing customers, only regarding similar products or services, while a clear opt-out option should be available. Furthermore, EU Member States hold discretionary power over unsolicited direct marketing communications that fall outside the scope of Article 13. Non-automated calls with human intervention constitute such an exception that falls under national regulatory competence. The above provisions of the ePrivacy Directive apply to natural persons as data subjects, while the protection of legal entities or subscribers other than natural persons is reserved for national discretion. Articles 6 and 9 of the ePrivacy Directive regarding traffic and location data may become relevant should the above marketing also include such data.

National implementation: Greece

Due to the nature of the ePrivacy Directive requiring national implementation, differences in the transposition into national law created compliance complexity across the EU Member States. Greece implemented the Directive into Law 3471/2006 on the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector and Amendment of Law 2472/1997 (the Electronic Telecommunications Law), as amended to accommodate Directive 2009/136/EC and the GDPR. The Electronic Telecommunications Law constitutes a rather strict transposition of the ePrivacy Directive.

Regarding unsolicited communications, the Greek Electronic Telecommunications Law appears stricter in exercising its discretionary powers. Particularly, while the relevant provisions of the ePrivacy Directive were transposed in an identical manner, legal entities and, in general, non-natural persons were granted the same exact protection as that enjoyed by natural persons. The differentiation between automated and human direct marketing was preserved, meaning that for non-human marketing, an opt-in system is in place, while for human-induced marketing, the opt-out clause should be available. Similarly, a soft opt-in system is in place in the case of direct marketing communication with previous customers for related products, meaning a right to object should be granted both at the time of collecting the contact details and each time a message is sent to the customer. While the Electronic Telecommunications Law requires verbal consent, the same law refers to the GDPR for the conditions of consent, which does not require that it be in a verbal manner. The ePrivacy Directive merely refers to the predecessor of the GDPR, i.e., Data Protection Directive 95/46/EC, and appears to require full harmonization in the area of consent. An interpretation consistent with EU law would consider consent valid even when it is merely inferred from the conduct of the user, without it being explicit.

The Electronic Telecommunications Law incorporated the provisions of the ePrivacy Directive that regard cookies in a similar manner. In this regard, the Hellenic Data Protection Authority (HDPA) issued recommendations on the compliance of data controllers with specific legislation on electronic communications (available in Greek here). The recommendations focused on the granting of consent for the operation of cookies, which, among others, requires an affirmative move by the user (scrolling is not adequate).

As to the processing of traffic data, the Electronic Telecommunications Law incorporated the ePrivacy Directive similarly. The HPDA, in its 71/2017 Decision, interpreted the above law and the exceptions to the requirement for prior consent. While in this case, the processing of traffic data is valid without prior consent, the user/subscriber should be duly informed (in this respect, a pre-recorded notice prior to the commencement of a telephone conversation that is about to be recorded should be adequate). Furthermore, in its 4/2022 Decision, the HDPA examined the issue of traffic and location data processing by a public service provider regarding fault detection and management. The HDPA found that while fault detection is considered a valid legal basis for traffic data processing under Recital 29 of the ePrivacy Directive, the latter should be carried out in accordance with personal data processing minimization requirements. On Decision 38/2022, the HDPA found the public service provider liable for not keeping up with the duty of security as demonstrated both in the ePrivacy Directive and the Electronic Telecommunications Law, meaning the provider did not take measures to prevent fraud incidents against its users. Even though the HDPA did not examine the validity of processing traffic data for fraud prevention purposes, the intensity of the duty of security as interpreted in the above decisions could justify a limited processing of data.

Conclusion

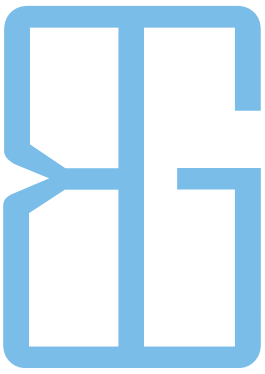
While providing a stepping stone for the effective regulation of communications at a European level, the ePrivacy Directive, mostly due to its nature and its transposition into national law, created a rather complex regulatory framework.

The ePrivacy Regulation, which was expected to resolve the said variations of legislation across the EU and impose a unified regime complementing the GDPR, was withdrawn by the European Commission in February 2025.

Authors:

Popi Papantoniou - Senior Associate
email: p.papantoniou@bahagram.com
Konstantinos Psevdos - Trainee Lawyer
email: k.psevdos@bahagram.com
Bahas, Gramatidis & Partners, Greece

1. Article 29 Data Protection Working Party, Opinion 2/2008 on the Review of the Directive 2002/58/EC on Privacy and Electronic Communications
2. Case C-673/17, Judgement of the Court (Grand Chamber) of October 1, 2019
3. Article 29 Data Protection Working Party Opinion 13/2011 on Geolocation Services on Smart Mobile Devices



BAHAS, GRAMATIDIS & PARTNERS LLP

Tel.: **+30 210 33 18 170**

email: **law-firm@bahagram.com**

Website: **www.bahagram.com**

Address: **26 Filellinon street, Athens 10558, Greece**