Privacy

UOC
Universitat Oberta de Catalunya
www.uoc.edu

Index

1. Privacy – the protection of personal data

The processing of data that identifies people – or "personal data" – is necessary for the provision of the vast majority of information society services. Think of the parties to a contract or the names of passengers for an electronic ticket, the email address of users registered with web platforms, etc. What is often unnecessary is the extent of personal data processing carried out, in terms of the data gathered, the uses made of such data or data transfers to third parties.

Example

For example, many of us receive unsolicited emails or telephone calls, often as a result of the illicit use of our personal contact details (e.g. which have been provided to another telecommunications operator or to the same operator for another purpose, such a billing).

This has led to significant abuses and strict regulation within the EU on the use of personal data.

In this module we will consider the protection and control of the use of personal data within the European Union, both generally speaking and in the context of electronic services and communications.

First we introduce the concept of privacy and its legal framework (which establishes the obligations of companies and the rights of individuals), and then we will discuss how information society services can be affected by privacy obligations.

The legal texts currently in force within the European Union are:

- Council of Europe Convention 108 of 28th January 1981.
- European Directive 95/46, related to the protection of private individuals in terms of the processing of personal data and the free circulation of such data (the *Data Protection Directive* or *DPD*). The aim of the Data Protection Directive is to reconcile privacy protection with the free flow of trade. In particular, it sets out requirements for the legitimate processing of personal data and requires that specific care is given to sensitive data.
- European Directive (2002/58/EC) concerning the processing of personal data and the protection of privacy in the electronic communications sector (*E-communications Directive*). The E-communications Directive provides specific rules for the processing of data related to provision of services over electronic communications networks (e.g. traffic and location data) and information security requirements in such networks.
- European Directive 2006/24/CE on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks (*Data Retention Directive*).

- National implementations of the privacy Directives, such as:
  - Spanish Organic Law 15/1999, on the Protection of Personal Data (the LOPD) and General Law on Telecommunications.
  - UK Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.
  - French "*Loi Informatique et Libertés*", 1978.

The Data Protection Directive came into force on 13 December 1995 and the deadline for implementation into each European Economic Area (EEA) Member State's national law was 24 October 1998. Member States interpret the Directive in slightly different ways, so when considering data protection issues, attention should be given to the national data protection legislation passed in the country concerned (as well as the Data Protection Directives).

Supplementary content

For EU legislative and case law references, see the European Commission site.

2. Basic concepts

Privacy protection regulations are designed to guarantee and protect personal data, public freedoms and the fundamental rights of private individuals, especially their right to personal and family honour and privacy.

There are requirements relating to the quality of the data and the legitimacy of the data processing. The Data Protection Directive also provides for extensive individual rights, not least the rights of access and rectification, and restricts trans-border data flows outside the EEA to those states without adequate protection. It also significantly strengthens security requirements for processing.

There are a number of specific exemptions and restrictions set out in the Data Protection Directive. These are not dealt with in any detail in this report. Suffice it to say that the scope of the principles relating to the quality of the data, information to be provided to the data subject, right of access and the publicising of processing may be restricted in certain circumstances. Such circumstances include the interests of national security, public security, the prosecution of criminal offences, important economic or financial interests of a Member State or the EU or the protection of the data subject.

2.1. Key definitions

In order to understand the legal framework of privacy, it is important to consider the following basic concepts:

- **Personal data**: any information relating to an identified or identifiable natural person ("data subject"). There is a sub-category of data that is especially protected (ideology, religion and beliefs, racial origin, health, etc.).
- **Files/filing system**: Any organised set of personal data, irrespective of its form or modality of creation, storage, organisation and access. This can extend to non-automated files (on paper) and to any type of personal data prone to handling.
- **Processing**: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **Data Subject**: The private individual owner of the data that is subject to processing.
- **Data Controller**: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (what, who, how, when

and where). The data controller is liable administratively, civil and potentially criminally, for potential infringements of privacy laws.

- **Data Processor**: The person who, either alone or in conjunction with others, processes data on behalf of the data controller. A common example is where an organisation appoints a third party IT company to provide data processing services to that organisation on an outsourcing basis.
- **Data Protection Agency**: a national authority with power to sanction is set up in order to guarantee the protection of personal data and to keep notified file registers (e.g. the Spanish *Agencia Española de Protección de Datos* or the *Information Commissioner* in the UK, *CNIL* in France).

As examples of files containing personal data, one could cite any set of data such as the medical histories of a doctor's patients (on condition that they are arranged following logical criteria) or the profile of users of a website (clients, registered individuals, etc.). It doesn't matter whether the data "format" is physical or electronic, nor is it relevant (in principle) whether it is subject or not to automated processing.

2.2. Roles

As we can see from the definitions, one of the key decisions in analysing data protection responsibilities is determining the status of the parties involved. In particular, this involves deciding which parties are data controllers and which parties are mere data processors. The *data subject* is the person whose data is being processed.

Data Controllers have the responsibility for ensuring compliance with data protection legislation, both at a national level and with the Data Protection Directive. Determining the status of the parties is not always so clear cut. In some circumstances, for example in joint ventures where there may be a number of organisations purporting to operate as a single entity, it may be more suitable for those organisations to act as joint controllers of the personal data.

Data Processors process data on behalf of the Data Controllers, and are subject to certain obligations, particularly as to security.

The E-communications Directive introduces two additional roles: the *public electronic communications network provider* and the *public electronic communications service provider*. These actors are responsible for the processing of traffic and location data, which will be explained in further detail below.

- The *public electronic communications network provider* operates the public electronic communications network (defined in Telecommunications Framework Directive) to include the operators of the relevant network infrastructure regardless of the technology used, made available wholly or mainly for provision of electronic communications services to the public (e.g. not enterprise networks and other internal systems).

- The *public electronic communications service provider* offers electronic communications services to the public, being generally speaking the "conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting". This excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services and information society services that we have commented on before.

These roles include traditional telecommunications operators who provide both the networks and the services on the network (fixed line and wireless voice and data carriers, e.g. telephone companies and internet access providers).

In relation to these services, the E-communications Directive introduces the concepts of "subscriber" referring to the person or entity which subscribes to electronic communications services, and "users", being the end-users of such services. The users may be data subjects under the Data Protection Directive.

2.3. Data processing

Privacy laws generally apply to the processing of personal data by automatic means (e.g. a computer database of customers) and data contained in or intended to be part of non automated filing systems (i.e. traditional paper files) and to any form of subsequent use of such data by the public and private sectors.

In some jurisdictions, certain categories of personal data are excluded from protection:

- Files held by private individuals in the course of their exclusively private or domestic activities (for example a personal agenda).
- Professional contact details, on condition that they refer to the company where the interested party works (name and surname, telephone, fax number, business address and electronic mail).
- Files related to national defence and the protection of the State, terrorism and serious forms of organised crime.

2.4. Territorial application

The general rule is that a data controller who is established in an EEA state must abide by the national law applicable to the place in which it is established. If the data controller has establishments in more than one EEA state he must follow the relevant national law for each establishment. Those laws will also apply to data controllers outside the EEA when processing is carried

out using equipment within the territory. This gives rise to certain questions with respect to online processing of personal data by a controller established outside the EEA.

> Thus the Spanish "LOPD" will apply to processing carried out on Spanish territory in the context of the activities of an establishment belonging to the data processor in Spain or in the European Union, or when the data processor is not established on Spanish territory but Spanish legislation applies in accordance with Public International Law. Regulatory security obligations apply to third party data processors on Spanish territory.

3. General principles

The Privacy laws establish certain general principles that must be observed with regard to the processing of personal data.

Generally speaking, as explained above, in order to process personal data lawfully, the data controller must identify a ground which justifies the processing. The criteria for lawful processing depend on the kind of data that is processed, i.e. general personal data, sensitive data, communications traffic or location data. These criteria aim at a somewhat broader principle of minimalism, i.e. that the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data are collected and further processed. This principle is also reflected in the strict rules on processing location and traffic data.

- **Data quality**. Article 6 of the Data Protection Directive sets out the three data quality requirements which shall be determined according to the specific case in question. These state that personal data must be:
  (a) Adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed (Article 6(c));
  (b) Accurate and, where necessary, kept up to date (Article 6(d)); and
  (c) Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were collected or for which they are further processed (Article 6(e)).

- **Purpose**. In addition, there is a purpose requirement. Article 6(b) states that "personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". Personal data may not be used for purposes that are incompatible with the reason for which it has been gathered and when the designated purpose has been fulfilled, it must be cancelled or destroyed.

  "Yahoo! uses information for the following general purposes: to personalise the advertising and content you see, based on the details given by you at registration and your activity at Yahoo!, fulfil your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients. You agree that Yahoo! may transfer your personal information for the general purposes set out above to any Yahoo! group company worldwide." Yahoo.co.uk Privacy policy, March 2010.

- **Information** (Art 10). Data subjects must be informed beforehand expressly, clearly and unequivocally of (a) the identity of the controller and of his representative, if any, (b) the purposes of processing for which the data are intended; and (c) any other information necessary to guarantee fair processing, having regard to the circumstances. In practice, information should be provided as to whether or not it is compulsory to provide the data, and how to exercise rights of access, rectification, cancellation

and opposition. If this information is not provided when the data is collected, then it must be provided later when processing is carried out (e.g. where the data have not been collected directly from the data subject).

In practice, the information is generally provided in the form of a data protection notice, which can be given to the data subject via application forms, terms and conditions, by telephone or on a website. By using an appropriately worded data protection notice, an online business can ensure that there is consent from visitors to its website to allow the business to build a valuable contacts database and market the visitors.

- **Data subject consent** (Art 7): The processing of personal data will require the informed, unequivocal, express or tacit, consent of the data subject, given freely (i.e. within the possibility to refuse), unless the law states otherwise (in other words, a legal authorisation, e.g. by court order). The processing of data that is especially protected requires express consent in writing. Certain categories of data or processing do not require consent, for example, data gathered from sources accessible to the public, data in commercial or employment contracts, or when processing is "necessary" to comply with a legal requirement, to protect the vital interests of the data subject (e.g. medical data) or for the *legitimate interests* pursued by the controller.

  This last ground is particularly useful to avoid the requirement for express consent, however some European jurisdictions (e.g. Spain) have not implemented this part of the Data Protection Directive, for constitutional reasons, which greatly limits the processing purposes that can be legitimised there. Relying on this ground is subject to challenge by a data subject who can show that processing is nevertheless prejudicial to his rights or freedoms or legitimate interests.

- **Confidentiality**: Both the data controller, and the data processor, as well as any other party intervening in any phase of the data processing, are obliged to professional secrecy in relation to the data and to maintain secrecy.

- **Data communications**: Subject to several exceptions, any communication or transfer of data to a third party requires the prior authorisation of the interested party.

In addition, the laws establish that it is generally forbidden to process "sensitive" personal data, i.e. that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and information concerning health or sex life, unless consent has been granted or in other specified circumstances.

4. Rights and obligations

As a result of these principles and other dispositions of the laws, the data subject benefits from various rights and the data processor is subject to a series of obligations.

4.1. Data subject rights

Data subjects have the following rights:

- To receive the abovementioned information at the time that the data is gathered (see above).

- To access, rectify and cancel such data, with a view to maintaining the accuracy of the data, rectifying or cancelling it when it is incomplete or inexact, inadequate or excessive for the purpose.

  The right to access is one of the most important rights available to data subjects under the Data Protection Directive. An individual may request access to all personal data of which he or she is the subject and which is being processed by the controller. In some jurisdictions, the controller may require the data subject to pay a maximum fee, (in the UK it is £10, however in Norway there is no fee imposed), to make the request in writing and to provide enough information to identify and verify the identity of the data subject making the request.

- To object and oppose processing of his/her data, when there are legitimate justified grounds relating to a specific personal situation and in particular to processing of personal data which the controller anticipates being processed for the purposes of direct marketing (and must be informed and given the right to object if data is disclosed to third parties for these same purposes).

- To contest any administrative or private action that involves an assessment of one's behaviour on the basis of the automated processing of one's personal data.

- In addition, where there is a general register of data files (Data Protection Agencies), the data subject is usually granted the right to consult the register free of charge.

Example

An example of an automated decision is where a financial services company uses an automated system to target, select and, more importantly, reject customers for particularly good credit offers.

Every person has the right to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.

4.2. Data controller and processor obligations

The data controller is subject to various obligations, the main ones being:

- To observe the general principles of data protection.
- To notify and register the data files with the Data Protection Agencies before carrying out any processing (Member States may dispense with this in certain circumstances). The Data Protection Directive (DPD) sets out certain information that must be notified, including the name and address of the controller, the purpose of processing, categories of data subject, categories of data, recipients of the data, details of transfers abroad and details of any security measures to be taken.
- To provide the interested party with the information mentioned above and to obtain their consent when necessary.
- To guarantee the procedures that allow data subjects to exercise their rights of access, rectification and cancellation.
- To document relationships with third parties intervening in the processing and, in particular, to ensure data processors only access data pursuant to a contract (see below).
- To implement the security measures of a technical and organisational nature necessary to guarantee the safety of the data under processing (see below).

A data processor must also fulfil the obligations included in the data processing contract: to carry out the activity on behalf of the data controller and to process the data in accordance with the instructions received. In the event of breach the obligations applicable under the privacy laws, the data processor will respond personally for any breaches committed.

5. Access to data and data transfers

5.1. Access by data processors

"Access to data" is understood to mean when a third party accesses the data in order to provide a service to the data controller. This third party is referred to as the "data processor". Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller.

Data processors

There are many examples of "data processors". Basically, it refers to the majority of information technology service providers that access or can access their clients' data:

- Data processing centres (outsourced).
- IT service providers (IT support, helpdesks, etc.).
- Customer care centres (which access user data).
- Companies providing web services, hosting and even data or email processing services (Amazon Web Services, Google Apps).
- Paper disposal companies.

The relationship must be governed by contract (often called an "Art 17 contract", under Article 17 of the DPD), which must be in writing and set out what the processor may or may not do with the personal data, including what security measures should be taken to safeguard the data. In particular, the data processor must implement the security measures indicated by the data controller.

Supplementary content

Controllers should reserve for themselves the right to audit processors to ensure compliance with the contract.

5.2. Data Transfers

Data transfers are not defined in the Directive, however Member States have generally provided that a transfer of data is any communication of personal data to a person other than the interested party, as distinct from an "access" to data as we have discussed above.

Data transfers

Typically, there is a transfer when data is transferred between a subsidiary and a parent company, from an HR consulting firm to its clients, from a doctor to a hospital or medical insurance company, or when marketing databases are sold (list of email addresses, etc.).

Personal data may only be transferred for the fulfilment of purposes directly related to the legitimate functions of the assignor and assignee and, with several exceptions (legal authorisation, etc.), must always have the prior informed consent of the interested party.

5.3. International data transfers (outside the EEA)

The concept of international data transfer covers both access to data by a data processor as well as its communication to third parties outside the EEA (EU Member States together with Iceland, Liechtenstein and Norway). Note that the mere transit of data via internet servers outside the EEA (email, web pages) does not count as a data transfer.

> Following the ECJ decision in the Swedish case against Lindqvist (C-101/01) in November 2003, data is not "transferred" to a third country where an individual in a Member State merely loads personal information onto a website that is hosted in that State or another Member State, so that the information can be accessed by anyone who connects to the internet.

As a general rule, the international transfer of data is only allowed when the destination is a country that ensures an "adequate level of privacy protection", i.e. offering the same level of protection as that provided by the DPD (article 25 DPD). This includes by default the EEA members, and also any other country approved by the European Commission (or an applicable Data Protection Agency) due to providing an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

> The countries approved to date are: Argentina, Canada, Hungary, Switzerland and the UK Island of Guernsey (and the US under the principles of "Safe-Harbour" and the transfer of Air Passenger Name Records to the United States' Bureau of Customs and Border Protection).

International transfer is also allowed in some other specific cases, for example, when (a) the recipient has signed a contract guaranteeing similar levels of data protection or (b) transfers between members of a business group that establishes a suitable internal policy for the protection of privacy (Binding Corporate Rules).

The availability of contractual safeguards is important, enabling data processors or controllers in third party countries to sign contracts with data controllers in the EEA (on the basis of the approved model clauses provided by the Commission) for the processing of data outside the EEA.

> Decisions 2001/497/EC and 2002/16/EC (now Commission Decision of 5 February 2010, C(2010) 593) set out standard contractual clauses for the transfer of personal data to third countries (data controller to data controller and data processor, respectively). A further Decision was passed in 2004 which introduced an alternative set of standard contractual clauses for the transfer of personal data to third countries.

Article 26 of the Data Protection Directive sets out a number of derogations (i.e. exceptions) to the aforementioned prohibition, so that transfers to third countries may be permitted where:

(a) The data subject has given his consent unambiguously to the transfer;
(b) The transfer is necessary for the performance of a contract between the data subject and the controller;

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

(d) The transfer is necessary or legally required on important public interest grounds or for the defence of legal claims;

(e) The transfer is necessary to protect the vital interests of the data subject; or

(f) The transfer is made from a public register.

The most commonly used of these derogations is (a) consent. Consent must be specific and informed. This means the individual must know and understand what such consent will amount to. Data subjects should be informed of the reasons for the transfer and the countries involved. In the data protection notice, controllers will often draft the notice widely and in particular will state that transfers to third countries may take place as a way of extracting consent from the data subject to such processing.

6. Security obligations

The data controller and, where applicable, the data processor, are obliged to implement appropriate (security) measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Supplementary content

For example, websites storing user data should implement measures to prevent unlawful access (hacking).

Google Privacy Policy, March 2010

"Information security. We take appropriate security measures to protect against unauthorised access to or unauthorised alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorised access to systems where we store personal data."

The Data Protection Directive does not predicate any particular measure and the member states of the European Union have taken different approaches to the issue, from self-regulation (UK) to detailed compulsory measures (Spain).

Under the Spanish Data Protection Laws, three levels of protection are established according to the type of information handled. The basic level applies by default to any personal data file, whereas the medium level applies to files containing data related to administrative or criminal violations, the Tax Authority, financial services, and credit ratings; and the high level applies to files containing data regarding the ideology, religion, beliefs, racial origin, health or sex life and data gathered for police purposes without the affected party's consent.

The different levels of safety involve obligations that are increasingly burdensome for implementation by the data controller and any processor (Security Manager). The basic obligations include preparing a security document and a register of incidents as well as defining the functions of the people with access to the data. Plus, for medium and high levels, a periodic (technical-legal) audit of the security measures implemented for the high level must take place, carrying out backup copies and encoding data transmissions.

7. Regulatory supervision

The DPD provides that the national Data Protection Agencies (supervisory authorities) must have certain powers to regulate the processing of personal data. This includes:

- Investigative powers, such as access to data processing operations and the collection of all the information necessary for the performance of its supervisory duties.
- Powers of intervention (delivering opinions before processing operations are carried out, ordering the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, of warning or admonishing the controller).
- The power to engage in legal proceedings where the data protection provisions have been violated.

National laws have provided these powers, and included powers to fine data controllers and processors for breach of the privacy obligations.

Spain

In Spain, the LOPD systematises the potential violations of the Law, classifying violations related to the protection of personal data. While there is no exhaustive list, the Agency can sanction any breach of the data subjects' rights (informed consent, rights of access, rectification and cancellation), lack of collaboration on the part of the Agency, lack of compulsory notifications or the creation, processing, communication, transfer and maintenance of files without observing the terms of the law. Breaches can entail fines between 600 and 600,000 Euros (per breach).

Various sanctions have been published, despite their alleged secrecy:

- In 2000,) a TV company Zeppelín was fined 1.1 million Euros for disclosing data on candidates for the Big Brother programme (this has been appealed).
- In 2001, Telefónica de España and Telefónica Data were fined 841,420 Euros for exchanging their client data.
- In 2002, the company Inlander had to pay 300,000 Euros for having its server installed in the United States.
- In 2008, the collecting society "SGAE" was fined 60,101 Euros for recording a wedding (to collect evidence of non-payment of levies).
- In 2010, Citybank España was fined 60,101 Euros for sending communications without consent (to one person!).

8. The legal framework for data privacy in other jurisdictions

Outside of Europe, we observe that due to the effect of these obligations and, especially, those relating to the international transfer of data, most commercial partners of European countries are almost "obliged" to establish similar legal frameworks for the protection of privacy. We would mention Canada, Switzerland and Argentina, which have been approved by the European Commission, but also Japan or Australia.

The United States is a special case, which has much less privacy protection than Europe, and which is organised by sectors: especially, for banks and financial services and the health sector. In order to allow the transfer of data from the EU, the US has established a quasi-private regime, by means of the Safe Harbor agreement of July 2000.

Safe Harbor

The decision by US-based organisations to comply with the Safe Harbor Privacy Principles is entirely voluntary. Organisations need to self-certify annually to the US Department of Commerce and state in their published privacy statement that they adhere to the principles. The Safe Harbor Principles impose obligations with respect to security and the appointment of data processors that are generally equivalent to those set out in the Data Protection Directive. US organisations can also meet the adequacy requirements of the Data Protection Directive if they include the Safe Harbor requirements as the substantive privacy provisions in written agreements with parties transferring data from the EU.

To date, approximately 2,000 US companies have signed the agreement. Others have signed standard contracts undertaking to protect the data appropriately.

9. Privacy in the sector of electronic communications

New technologies, in particular internet and email, must fulfil certain requirements in order to guarantee the right to privacy. The amount and intensity of communications as well as the nature of data transmitted can be a risk for people's privacy. Therefore, to improve people's confidence in the use of telecommunications, a series of rules have been established imposed on electronic network and service providers. These were established by the E-communications Directive and the Data Retention Directive.

9.1. Telecommunications secrecy

Member States within the EU generally impose obligations of confidentiality and secrecy in respect of telecommunications.

The three basic principles are:

- **The secrecy of communications**: the confidentiality of communications carried out through public electronic communication networks must be guaranteed. In particular, it is prohibited for people other than users to listen to, intercept or store communications without the prior consent of users or a court order.
- **Interception**. The laws develop the principles for the interception of electronic communications by agents of the public administrations. Data protection confidentiality obligations are only restricted in order to carry out investigations into criminal activities or to guarantee national security, public defence and safety, in conditions where the lifting of confidentiality constitutes a "necessary, proportionate, and appropriate measure in a democratic society".
- **Encryption**. The encryption of data circulating on electronic communication network is normally allowed (e.g. Skype encrypts messaging), however certain national laws also allow the authorities to demand handover of the encryption keys.

The E-communications Directive reiterates these basic principles, providing that Member States must ensure the confidentiality of communications made over a public electronic communications network. They must, in particular, prohibit listening, tapping and storage of communications by persons other than users without the consent of the users concerned.

9.2. Electronic communications

9.2.1. Traffic data and Location data

The E-communications Directive defines:

- **Traffic data** as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". The definition covers data such as call data, addressing or numbering data (e.g. IP-addresses or phone numbers), data relating to the routing, duration, time, protocol used, or data generated for the purpose of billing.

- **Location data** as "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".

- Traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Processing of traffic data may only take place to the extent and duration necessary to fulfil certain specified purposes: subscriber billing and interconnection payments, marketing electronic communications services or providing value added services provided the user or subscriber has given prior consent; or fraud detection, traffic management and handling customer enquiries.

  Service providers must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing. This information must be provided before obtaining consent to marketing electronic communications services or providing value added services. Users or subscribers shall also be given the possibility to withdraw their consent for the processing of traffic data for these purposes at any time.

  The Directive also sets restrictions on the entities that are allowed to process traffic data. Traffic data may only be processed by persons acting "under the authority" of electronic communications network or service providers (i.e. internet access providers, mobile operators, etc.).

  This requirement suggests that the persons involved in the processing of traffic data either have to be employed by the network or services provider, or that third parties must be appointed as a processor in accordance with the Data Protection Directive.

- Location data (other than traffic data) can only be processed if it is made anonymous or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision of any services. The service provider must inform the users or subscribers, prior to obtaining their consent of: the type of location data which will be processed; the purposes and duration of the processing; and whether the data will be transmitted to a third party for the purpose of providing the value added service.

  Users or subscribers must be given the possibility to withdraw their consent for the processing of location data at any time and also, using a simple means and free of charge,

to refuse temporarily the processing of such data for each connection to the network or for each transmission of a communication.

Restrictions similar to those applicable to traffic data are imposed on the entities and persons that can process location data (e.g. persons involved in the processing of location data either have to be employed by the network or services provider, or that third parties must be appointed as a processor in accordance with the Data Protection Directive).

9.2.2. Security requirements

The E-communications Directive sets out additional security measures in relation to the processing of personal data in the electronic communications sector. The provisions of the Data Protection Directive are reinforced, as providers of publicly available electronic communications networks must take appropriate technical and organisational measures to safeguard the security of its services.

The E-communications Directive also regulates the use of cookies (hidden information exchanged between an internet user and a web server that is stored in a file on the user's hard disk, which is useful for monitoring a net surfer's activity). Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. To that end, notice of uses of cookies must be given and users must be able to decide not to accept cookies, except where the cookie is essential to deliver contracted services.

UK Information Commissioner website

"We use Google Analytics to help analyse use of our website. This analytical tool uses 'cookies', which are text files placed on your computer, to collect standard internet log information and visitor behaviour information in an anonymous form. The information generated by the cookie about your use of the website (including your IP address) is transmitted to Google. This information is then used to evaluate visitors' use of the website and to compile statistical reports on website activity for the ICO. To find out more about cookies, including how to control and delete them, visit www.aboutcookies.org/".

9.3. Data Retention

In March 2006, Directive 2006/24/CE was adopted regarding the preservation of data generated or processed in relation to the provision of services of electronic communication of public access or of public communication networks. The purpose of the Directive was to harmonise the rulings of Member States regarding the obligations of electronic communication service providers related to data preservation.

This Directive establishes the obligation to preserve certain categories of data by electronic communications service providers. The aim is to guarantee that such data is available for purposes of investigating, detecting and judging violations.

The Directive defines:

- The categories of data that need to be preserved: e.g.
  - Data regarding travel and location of private individuals and legal entities.
  - The data listed as necessary for identifying a subscriber or registered user.
- The periods for the preservation of data (basically, 12 months).
- The storage requirements for preserved data (guaranteeing confidentiality).
- The regime for transferring the data to public authorities, following a court order.
- The principles that must be respected in terms of data security, in accordance with the DPD.

Supplementary content

The scope of application of the Directive excludes the content of electronic communications; including information consulted using an electronic communication network.

10. Conclusions: the impact of privacy on technological projects

One cannot underestimate the impact of data protection regulations on technological projects. The obligations to inform and obtain the consent of the user and regarding data security are very cumbersome when there are millions of users involved. The prohibition of international data transfers determines where data processing, outsourcing or customer care services can be located, (for example, in Argentina or Canada, countries approved by the European Commission).

The viability of certain projects has been questioned due to the cost of fulfilling privacy obligations and restrictions regarding the use of personal data.

It is fundamental to carry out an impact study of the privacy obligations on the project's systems, processes and costs during the project's analysis, as well as to determine who is responsible for implementing the corresponding obligations (data gathering with prior information to the user, etc.) and notifying files to the Data Protection Agencies.

Very briefly, this analysis implies:

- Determining the category of personal data processed by the project's systems.
- Identifying who is responsible for these data (the person who determines the purposes of processing, the "owner" of the data).
- Establishing the obligations to inform, obtain consent and prove it (acceptance registers, etc.) and how they are implemented (web privacy policies, client documentation, etc.).
- Establishing the levels of security to be implemented, their implementation and corresponding cost.
- Defining the processes to respond to access and cancelation requests by interested parties.
- Identifying third parties with access to the data (data processors – data hosting companies, outsourcing companies, software and technology maintenance services, etc.) and, where applicable, the transfers of data to third parties, which must be justified.