SECURITY MEASURES IN THE PERSONAL DATA PROTECTION RULES: TECHNOLOGICAL SOLUTIONS AND LEGAL ADAPTATION

Antonia Paniza-Fullana

Civil Law
University of Balearic Islands

Abstract. Several practical issues arise in the papers of the research group of ARES. So, this report analyzes some legal aspects about data protection and privacy; especially, security processing, dissociated data and security measures

Besides, this report presents some legal aspects of the Location Based Services that is another issue in the ARES group.

1 Legal Framework

1.1 In General

Some important legislation related to data privacy is:

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
2. Data Protection Act (L.O. 15/1999, December 13th).
3. Real Decreto 1720/2007, December 21st, approving Regulation developing Data Protection Act.

1.2 Article 11 Data Protection Act (LOPDP): Dissociated Data

In general, personal data only can be communicated to third parties with the previous consent of the user. In general, this consent is not necessary in some cases: in the cases established by the law; personal data from public resources; data processing form a contractual relationship or when the destinatary are judge or some public statements; for statistical or historic purposes, etc.

Besides the user previous consent, he must know the purposes of the processing data. This consent is revocable by the user. In the case of dissociation processing that not allowing identification of the data subject is not necessary the consent of the user. Personal data is defined as any alphanumeric, graphic, photographic, acoustic or any other type of information pertaining to identified or identifiable natural persons. An identifiable person is defined as one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In the case of dissociation procedures it has to be impossible to relate a specific person with his data. Article 5.1.e) Regulation 1720/2007 (RLOPDP) defines "dissociated data" as data that does not permit identify the user[1]. So, only in this case it is not necessary accomplish all the requirements of article 11 of Data Protection Act.

In this way whereas article 26 of the Directive 95/46/EC establishes that "the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, it should be taken into account all the means likely reasonably to be used either by the controller or by any other person to identify that person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable".

On the other hand, codes of conduct may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.

2 Security measures and data protection.

European and Spanish rules demand security measures in the context of data processing. These rules are:

1. Article 17 Directive 95/46/EC: Security of processing: "1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against

[1] Vid. Report of Spanish Agency of Protection Data 37/2010.

accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: - the processor shall act only on instructions from the controller, - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form".

2. In Spain, article 9 Data Protection Act is about the security of the data and Real Decreto 1720/2007, December 21st, that approve the Regulation developing Data Protection Act establishes the regulation of security measures (articles 79 and next).

The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

There are three levels of security: basic, medium and high level. The classification depends of the type of data that is processing. All the processing of personal data is obligated to fulfil the security measures qualified as basic. Articles 2 and 3 list the cases that is necessary implant medium and high security measures. All the personal data filing must include security measures in the basic level. Personal data filing that re-

quire security measures medium level are: data about administrative or criminal infractions, Treasury, financial services and personal data about solvency and credit. Personal data that need technical measures of high level are sensitive data: data about ideology, religion, health, etc.

Data Protection regulation lists different security measures. They depend on the type of data that will be processed. Security measures about: access control; access authentication; incident register; copies, etc. (articles 89 to 104)[2].

Article 104 establishes the obligation to establish special security measures in case of transmission of personal data over a public network or wireless electronic communications: data (in case of high level protection) must be encrypted. This type of transmission involves particular security risks, e.g. the transmission could be intercepted by a third party.

Controller or processor must fulfil the "security document". In this document will be technical and organizational measures to protect personal data according to the law. Security document must contain everything related to the measures, standards and operating procedures, rules to be applied to ensure the security of personal data processing. It is an internal document mandatory for anyone who can access the data. (Model of security document of the Spanish Data Protection Act: `https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf`).

A consequence of a breach of the security rules is a serious infraction according to article 44.3 h) of Data Protection Act.

[2] Vid. GUARDA, P.: Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks, December, 2008. In Italy and in a very similar way in Spain: - Authentication credentials shall consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password; - Implementation of authentication credentials management procedures; - Use of an authorization system, that can allow the user to access to specific resource to pinpoint the authorization profile; - Implementation of procedures for safekeeping backup copies and restoring data and system availability (i.e. back-up copies), etc.

3 Specific applications: Legislation on privacy and location-based services.[3]

Location data are regulated in the article 9 of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

The requirements to use the location data by the service provider are:

- Location data relating to users or subscribers of public communications networks or publicly available electronic communications services can be processed when they are anonymous or with the consent of the users or subscribers.

- This data can only be processed to the extent and for the duration necessary for the provision of a value added service.

- Service providers must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

- Besides, users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

- The user or subscriber must continue to have the possibility, using simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication[4].

In the same way the Spanish Telecommunications Act (Act 32/2003, November 3rd) in the article 38.3 says: location data can only be processed when it is anonymous or if the provider has the consent of the user or subscriber. Location data can only be processed to the extent and for the duration necessary for the provision of a value added service and with

[3] Paniza-Fullana, A., Payeras-Capell, A, Mut-Puigserver, M., Isern-Deya, A.: Reflections on Privacy in New Location Based Services in Social Networks in IADIS International Conference. E-commerce 2011. Proceedings. Lisboa, 2011, pag. 211 a 214.

[4] Vid. Opinion Article 29 Working Group 13/2011 on Geolocation services on smart mobile devices

prior information about the purposes and duration of processing and for the added value service that will be provided[5].

4 Conclusions.

In the case of dissociation processing data it is not necessary fulfil all the requirements of personal data protection rules. But dissociation data means that it is impossible to identify the user.
Data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. It is very important the "security document". Every company have to adequate this document to the personal data that it processes (it is not the same a hospital or a company of financial services or others).
Security measures need to be reviewed on a regular basis to ensure that they are effective.
In the case of location data relating to users or subscribers of public communications networks or publicly available electronic communications services only can be processed when they are anonymous or with the consent of the users or subscribers.

References

1. Security document Spanish Data Protection Agency:`https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf`.
2. Guarda, P.: Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks, December, 2008.
3. Martnez, R. Las medidas de seguridad in Martnez, R. (Coord.): Proteccin de Datos. Comentarios al Reglamento de Desarrollo de la LOPDP, pages 89 a 119, Valencia, 2009.
4. Paniza-Fullana, A., Payeras-Capell, A, Mut-Puigserver, M., Isern-Dey, A.: Reflections on Privacy in New Location Based Services in Social Networks in "IADIS International Conference. E-commerce 2011. Proceedings. Lisboa, 2011, pginas 211 a 214.

[5] Vid. Spanish Agency of Protection Data Report 160/2004 about safety measures of data location files.