"This project has been funded under the HOME/2012/ISEC/AG. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein"

PROJECT Nº HOME/2012/ISEC/AG/4000004374

D7.2 Data Protection and Privacy Requirements

Start Date of Project : 01/01/2014 Duration : 24 months

PROJECT FUNDED BY THE EC DIRECTORATE GENERAL FOR HOME AFFAIRS	
Due date of deliverable	M15
Actual submission date	March 2015 (M15)
Lead partner	HI-Iberia
Participant(s)	MCC, MDX
Work package	WP7
Classification	PU
Version	V0.1
Total number of pages	22

DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and SAMi2 partners have endeavored to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this report (or any further consolidation, summary, publication or dissemination of the information contained within this report) and/or the connected work and disclaim all liability for any loss, damage, expenses, claims or infringement of third party rights.

List of Authors

Partner	Authors
Middlesex University	Dr. Carlisle George

Table of contents

List of Tables

Glossary

Acronym	Meaning
DLOPD	*Decree 17/2007 relating to Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*. (Royal Decree 1720/2007 relating to Organic Law 15/1999). Spain
LOPD	*Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*. (Organic Law 15/1999 on Personal Data Protection).

References

Laws and Regulations

Council Framework Decision 2008/977/JH on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector. Available at: http://polis.osce.org/library/f/2670/471/CoE-FRA-RPT-2670-EN-471

EU proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security, and the free movement of such data. Available at: http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/en/pdf

European Convention on Human Rights. Available at: http://www.echr.coe.int/documents/convention_eng.pdf (last accessed October 2015)

EU Directive 95/46/EC on Data protection. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Organic Law 15/1999 on Personal Data Protection (*Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal or LOPD*). Available at: http://www.legislationline.org/documents/id/9044

Royal Decree 1720/2007 relating to Organic Law 15/1999 on Personal Data Protection. Available at: http://www.davara.com/documentos/relacionados/proteccion/RD_1720-2007_english.pdf

The Charter of Fundamental Rights of the European Union. Available at: http://www.europarl.europa.eu/charter/default_en.htm

1 Introduction

The work presented in this deliverable D7.2 gives a summary of the main privacy and data protection requirements discussed in delivery D7.1.

The Table 1 identifies legal frameworks and the corresponding important legal considerations of each framework.

2 Table of Requirements

Privacy and Data Protection requirements	
Legal Framework	**Important legal requirements**
Human Rights	
European Convention of Human Rights.	***Right to respect for private and family life (Art 8)*** Everyone has the right to respect for his private and family life, his home and his correspondence, (Art 8).
Charter of Fundamental Rights of the European Union.	***Respect for private and family life (Art 7)*** Everyone has the right for his or her private and family life, home and communications,
European Union Data Protection legal Framework	
Charter of Fundamental Rights of the European Union	***Protection of personal data (Art 8)*** 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified
Council of Europe Recommendation R(87)15 regulating the use of personal data in the police sector	***Data Collection*** Data collection should be limited to what is necessary for police purposes (prevention of real danger or to suppress a specific criminal offence), except where specific national legislation provides otherwise. A data subject must be informed of data collected and stored about him/her without his/her knowledge if not

	deleted, as soon as there will be no prejudice to police activities. The collection of sensitive personal data (e.g. racial origin, religious beliefs, sexual life, political opinions) is not permitted unless absolutely necessary for a particular investigation
	Data Storage Data stored for police purposes should be limited to data that is accurate and necessary for the police to perform their functions. Categories of data stored should be distinguished: according to their degree of accuracy or reliability; and according to whether data is based on facts versus opinions or personal assessments. Data collected for administrative purposes which needs to be stored permanently should be a separate file from police data, and not subject to rules applicable to police data.
	Data use Data collected and stored for police purposes should only be used for these purposes.
	Communication of data Only permissible where there is a legitimate interest for the particular communication as provided for by an existing legal framework detailing the powers of the two bodies involved in the communication
	Rights of data subjects Data subjects have various rights (subject to exemptions) such as: the right of access to their police file; the right to rectify inaccurate data held in a police file; and the right of erasure of data that is excessive or irrelevant. Any refusal or restriction of these rights needs to be made in writing to the data subject who can appeal to the national data protection supervisory authority

	Length of storage and updating of data Data should only be kept for as long as necessary for the purposes for which they were collected.
	Data Security Appropriate physical and logical security measures must be taken to secure data and to prevent any unauthorized access, communication or alteration.
Council Framework Decision 2008/977/JH	Data should be kept accurate and erased when no longer required (Art 4).
	Time limits must be kept for the erasure and review of data (Art 5).
	Sensitive personal data (e.g. racial and ethic origin, sexual orientation, political opinions, religious beliefs, health information and trade union membership) should only be collected if strictly necessary (Art 6).
	Automated decision can only be made if authorized by law (Art7).
	The quality (accuracy, completeness) of data transmitted or made available for transmission must be verified and if incorrect data has been transmitted or data has been unlawfully transmitted then the recipient of the data must be notified (Art 8).
	Time limits on the retention (by the recipient) of data sent can be set by the transmitting authority, however they shall not apply if the data are required by the recipient for ongoing policing purposes at the time of expiry of the time limits set (Art 9).
	All transmissions must be logged and documented (Art 10)
EU Data Protection Directive (Directive 95/46/EC)	***Principles related to data quality (Art 6)*** (a) **Fair and Legal** - Personal data must be “processed fairly and lawfully”

	(b) **Purpose-Limited** - Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes…." (c) **Relevant** - Personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (d) **Accurate** - Personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard for the purposes for which they were collected or for which they are further processed, are erased or rectified." (e) **Time-Limited** - Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."
	Criteria for legitimate data processing (Art 7) (a) **Consen***t* - Personal data may be processed when "*the data subject has unambiguously given his consent*." The Directive further specifies that consent must be both informed and voluntary. (b) **Contract** - Personal data may be processed when "*necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."* (c) **Legal Obligations** - Personal data may be processed when *"necessary for compliance with a legal obligation to which the controller is subject."* (d) **Vital Interests** - Personal data may be processed when *"necessary in order to protect the vital interests of the data subject."* *(e)* **Public Interest** - Personal data may be processed when "*necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed."* *(f)* **Legitimate Interests** - Personal data may be processed when *"necessary for the purposes of the legitimate interests pursued by the controller or by the*

	third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Art 1(1).”
	Criteria for legitimate data processing of sensitive personal data (Art 8) (a) a data subject has given explicit consent, (b) processing is necessary for controller to meet legal obligations with respect to employment law, (c) processing is necessary to protect the vital interests of a data subject (or another person), and the data subject is physically or legally incapable of giving consent (d) processing is carried out by a non-profit organization whose aim is to advance an agenda related to one of the categories of sensitive data, (e) the data are manifestly made public by the data subject, (f) processing is necessary to establish or defend legal claims, and the processing is required by a health professional in the course of providing treatment or managing health-care services.
	Some important rights of Data subjects – **Right of Access** to obtain information regarding (Art 12a): (a) whether their personal data is being processed, (b) the content and source of any personal data undergoing processing, and (c) the purpose of any such processing. – **Right to correct**, erase, or block the transfer of inaccurate or incomplete data. (Art 12b) – **Right to “object at any time on compelling legitimate grounds** *relating to [their] particular situation to the processing of data relating to [them], save where otherwise provided by national legislation*.” Data subjects also have the right to object “*to the processing of personal data relating to [them] which the controller anticipates being processed for the purposes of direct marketing*.” *Art 16)

	– **Right not to be subjected to solely automated decisions** (Art 15).
	Obligations on Data Controllers **Notice to Data Subjects (Art 10)** Except where a data subject already has such information, controllers must provide the data subject with the following information: (a) the identity of the controller; (b) the purpose of the processing; (c) the recipients or "categories of recipients" of the data; (d) whether providing information is obligatory or voluntary (including an explanation of the consequences of failure to provide the information); (e) the existence of the right to access and correct personal data. **Notice to Data Protect Authorities (Arts 18 & 19)** Except where national law provides an exemption, controllers must provide the relevant data protection authorities with the following information prior to performing any automatic processing operation: (a) the name & address of the controller & any relevant representative (b) the purpose(s) of the processing; (c) a description of the category or categories of persons affected, and of the data relating to them; (d) the recipients to whom the data may be disclosed; (e) any proposed transfers to third countries; and (f) a general description of measures taken to ensure the security of processing
	Transfers of personal data to third countries (Arts 25 and 26) The Directive expressly prohibits the transfer of personal data to third (non-EU) countries except under limited circumstances. The exceptions to the general prohibition against transferring personal data outside of the EU fall into the

<table>
<tr><td></td><td>following categories: country-specific, business-specific or circumstance-specific.</td></tr>
<tr><td rowspan="3">Proposed EU Directive for law enforcement.

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security, and the free movement of such data (Version correct at 2nd October 2015)</td><td>Principles relating to personal data processing (Art 4(1))

Personal date must be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes.

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

[(ee)] processed in a manner that ensures appropriate security of the personal data.</td></tr>
<tr><td>Transmission of personal data (Art 6)

Personal data that is inaccurate, incomplete or no longer up to data must not be transmitted or made available.

If personal date is unlawfully transmitted or the data is incorrect then the recipient must ben notified immediately. This data must then be rectified, erased or restricted in accordance with Art 15.</td></tr>
<tr><td>Lawfulness of processing (Art 7)

Lawful processing is any Processing carried out under EU law or national law for the purposes set out in Art 1(1) i.e. “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security.”</td></tr>
</table>

	Processing of special categories of personal data (Art 8) The processing of special categories of personal data (e.g. racial/ethnic origin, religion, political opinions, trade-union membership, genetic data, health data, sex life) is prohibited unless: it is necessary, subject to safeguards to protect the rights and freedoms of the data subject and only if (a) authorized by Union law or national law, or (b) done to protect the vital interests of the data subject or another person or (c) the data being processed has already been made public by the data subject.
	Automated decision making including profiling (Art 9) Decisions based solely on automated processing including profiling that either results in an adverse legal effect for the data subject or significantly affects the data subjects is prohibited unless authorized by union law or national law which provides appropriate safeguards regarding the rights and freedoms of the data subject (including at least the right for the data subject to have human intervention on the controller),
	Rights of data subjects Under Art 10(a) the following must be made available to a data subject: the identity and contact details of the data controller; the purposes of the processing for which personal data is intended; and the right to make a complaint to the supervisory authority. **Right of a data subject of access** to data being processed about him/her and to obtain further information including: the purposes of such processing, to whom the data has been disclosed, and length of data storage among others (Art 12). There are various limitations to the right to access. These are given in Art 13 and include: "*(a) to avoid obstructing official or legal inquiries, investigations or procedures;* *(b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;* *(c) to safeguard public security;*

	(d) to safeguard national security; *(e) to safeguard the rights and freedoms of others*." **Right to rectification, erasure and restriction of processing (Art 15);** **Right to be notified of any personal data breach (Art 29).**
	Data Protection by design and default (Art 19) Appropriate technical and organisational measures based on current technology and cost of implemented, should be implemented (appropriate to the processing activity being carried out and its objectives) to meet the provisions of the Directive and protect the rights of data subjects.
	Records of personal data processing activities (Art 23) Each data controller must maintain a record of all categories of personal data processing activities under its responsibility.
	Logging (Art 24) In automated processing systems logs must be kept of the following processing operations (unless impossible to do so or it involves a disproportionate effort): collection, alteration, consultation disclosure, combination or erasure.=
	Security of data processing (Art 27) Data controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
	Notification of personal data protection breach to the supervisory authority (Arts 28) When a personal data breach occurs and it is likely to be of high risk to the rights and freedoms of data subjects, the controller must notify the supervisory authority not later the 72 hours after becoming aware of it. Where the

<table>
<tr><td></td><td>notification is given later than 27 hours, reasons for doing so must be given.</td></tr>
<tr><td></td><td>Communication of a personal data breach to the data subject (Art 29).

The controller must also inform the data subject (without undue delay) of any data breach that is likely to result in a high risk for his/her personal rights and freedoms.</td></tr>
<tr><td colspan="2">Spanish Data Protection Legal Framework</td></tr>
<tr><td>Organic Law 15/1999 (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal), (LOPD)

&

Royal Decree 1720/2007 relating to Organic Law 15/1999 (DLOPD)</td><td>Data Protection Principles

- <u>Data Quality</u>

Lawful basis need for processing data
There must be a lawful basis for processing data. LOPD Art 4(1), DLOPD Art 8(1)

Purpose limitation
Data should be processed for specific (or compatible) purpose(s) for which it was collected. LOPD Art 4(2), DLOPD Art 8(2), DLOPD Art 8(3),

Data minimization
The minimum necessary data required should be collected and kept. LOPD Art 4(4), LOPD Art 4(5), DLOPD Art 8(4)

Proportionality
Data processed must be adequate, relevant and non-excessive in relation to the purposes for which they are collected. LOPD Art 4(5): as above, DLOPD Art 8(4) as above.

Exercise of rights by data subjects. LOPD Art 4(6)

- <u>Transparency</u></td></tr>
</table>

	Right for data subject to be informed when collecting data. LOPD Art (5)(1), LOPD Art 5(4), LOPD Art 5(5). With regarding to the processing of personal data carried out in SAMi2, LOPD Art 5(5) provides an exemption for subject notification since generally it may not be possible to contact people whose personal data may be included in the text of tweets. SAMi2 will automatically collect thousands of tweets and it will be impossible to distinguish personal data from non-personal data in unstructured texts. Regarding law enforcement, Data subjects' right to information during data collection (LOPD Art 5), is not applicable if informing data subjects will hinder or impair public authorities in their duties, or where the following is involved: national defence, public safety, the prosecution of criminal offences or misdemeanors (LOPD Art 24). **Consent of data subject,** LOPD Art (6)(1), LOPD Art 6(1) **Exercise of rights by data subjects,** LOPD Art 4(6) **- Data with special protection** LOPD Art 7 details certain categories of data that need to be processed only with the explicit consent of the data subject. They include data relating to: ideology, political philosophy, trade union membership, religion, racial or ethic origin, sex life and beliefs. (LOPD Art 22(2) gives law enforcement special exemption from this provision). **- Security** LOPD Art 9(1) states that the controller (and processor) must take all necessary measures (technical and organizational) to: make sure that data is secure; prevent the alteration or loss of data; and the unauthorized

	processing or access to data. This must be done in the context of the state of the art of the technology, the nature of the data stored, and the risks (whether human action or physical or natural causes) to which the data is exposed. LOPD Title VIII addresses several provisions regarding security measures in the processing of personal data. **- <u>Secrecy</u>** LOPD Art 10: "*The controller and any persons involved in any stage of processing personal data shall be subject to professional secrecy as regards such data and to the duty to keep them. These obligations shall continue even after the end of the relations with the owner of the file or, where applicable, the person responsible for it.*" **- <u>Data disclosure</u>** LOPD Art 11(1): "*Personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject.*" LOPD Art 11(2) gives several exemptions to the consent required in LOPD Art (1) including "*when the data were collected from publicly accessible sources.*" *Access to data by third parties* LOPD Art 12: details the requirements for third party access to data.
	Rights of data subjects (note that <u>Law enforcement can deny subject rights to access, rectification and erasure based</u> on the reasons given in LOPD Art 23) – Right to object to assessments or acts/decisions, made based solely on data protection procedures, intended to evaluate personality or behavioural aspects (LOPD Art 13). – Right to consult the General Data Protection Register to verify that records of their personal data, purpose

	for their collection and identity of controller (LOPD Art 14). – Right of access to information about personal data – how it was obtained, has been or is being used and/or communicated to third parties (LOPD Art 15, DLOPD Art 27). – Right of rectification and erasure of personal data that is inaccurate, incomplete or processed in violation of data protection law (LOPD Art 16, DLOPD Art 31). – Right to object to certain kinds of processing: where consent is not required but there are legitimate grounds relating to personal circumstances; for advertising and direct marketing; to make decisions based solely on automatic processing of personal data. (DLOPD Art 34, Art 36). – Right to Indemnity/compensation for loss suffered due to violations of data protection law (LOPD Art 19).
	Public Sector files **Registration** Public authorities are required to undergo registration of their files (databases) in the Official State Journal or analogous regional publication, before processing data (LOPD Art 20). A registration must contain a description of: the purpose of the database and its intended use; persons or groups whose personal data will be gathered; how personal data will be gathered; the structure of the database; any surrender of personal data and planned transfer of personal data to third countries; public bodies responsible for the database; how subjects' rights will be addressed; and security specification (low, medium or high level). **Data disclosure between public authorities** LOPD (Art 21) prohibits disclosure of personal between public authorities to perform duties of a different nature or relating to different matters, except this is allowed by other legislation, or whether data are discloses for processing related to historical, statistical or scientific purposes.

	Files kept by law enforcement LOPD Art 22(2) limits the scope of personal data collection by the law enforcement where there is no consent from the data subject. This scope is limited to data required to safeguard public safety and prevent crime. Further the data must be stored in specific files established for this purpose and classified according to the degree of their reliability. Specially protected data described under LOPD Art 7 (i.e. data relating to ideology, political philosophy, trade union membership, religion and beliefs) can be collected and processed by law enforcement only when absolutely necessary for investigations, (LOPD Art 22(2)). LOPD Art 22(4) mandates that personal data collected for law enforcement purposes should only be kept for as long as necessary and then erased. **Exceptions to the rights to access, rectification and erasure.** Law enforcement can deny subject rights to access, rectification and erasure based on the following reasons LOPD Art 23: risks to state security, protection of third party rights/freedoms, and the protection of an ongoing investigation. Any denial of subject rights must be reported to the Direct of the Data Protection Agency or competent regional body. **Other exception to subjects' rights** Data subjects' right to information during data collection (LOPD Art 5), is not applicable if informing data subjects will hinder or impair public authorities in their duties, or where the following is involved: national defence, public safety, the prosecution of criminal offences or misdemeanors (LOPD Art 24).

Table 1 – Summary of privacy and data protection requirements