

Security Sensitivity Statement

This form is related to the Security Sensitivity Assessment procedure which will assure that no sensitive information will be included in the publications and deliverables of the MobilePass project.

Security sensitive information means here all information in whatever form or mode of transmission that is classified by Council Decision on the security rules for protecting EU classified information (2011/292/EU) and all relevant national laws and regulations. The information can be already classified, or such that it should be classified.

In practice the following criteria is used:

- Information is already classified
- Information may describe shortcomings of existing safety, security or operating systems
- Information is such, that it might be misused.
- Information that can cause harm to
 - o European Union
 - o a Member State
 - o society
 - o industry and companies
 - o third country
 - o citizen or an individual person of a country.

Publication identification

Title of the Publication: Deliverable WP1 / Deliverable D1.2 Data Handling Guidelines

Authors (Name / Affiliation): Sanneke Kloppenburg, UNU-MERIT, Irma van der Ploeg, UNU-MERIT

Type of the publication: Deliverable

Dissemination Level: PU



25.08.2014

Please fill in below:

This is: *pre-assessment* *final assessment*

List the input material used in the publication/deliverable:

1. See References, pg. 20

List the results developed and presented in the publication/deliverable:

- Data handling guidelines for research and development activities

The draft publication

is attached to this statement

can be found in link: <http://www.mobilepass-project.eu/dissemination>

This publication does not include any data or information that could be interpreted as security sensitive.

True

Not sure

If not sure, please specify what are the material / results that you are not sure if they are security sensitive? Why?

Date 28.10.2014

Signature of the Responsible Author:



Comments of the SSA Group

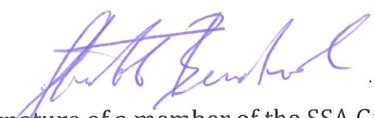
The publication can be published as it is.

Before publication the following modifications are needed:

- none

Date: 28.10.2014

On behalf of the SSA Group:



Signature of a member of the SSA Group
(STROJL BOROVNIK)



Project

Project Reference:
Project Short Name:
Call:
Funding Scheme:
Project web-site:

MobilePass

Grant agreement no. 608016
MobilePass
FP7-SEC-2013-3-2-3
Capacity Project
www.mobilepass-project.eu



Deliverable D 1.2

Data handling guidelines

Document

Deliverable No.:	1.2	Due Date:	2014-31-10
Issued by Partner:	UNU-MERIT	Actual Date:	2014-28-10
WP/Task:	WP1/T1.2	Pages:	20
Confidentiality Status:			

Authors

Main Authors

Name

Sanneke Kloppenburg
Irma van der Ploeg

Organization/Unit

UNU-MERIT
UNU-MERIT

Reviewed by

Belen Fernandez Saavedra	UC3M
Eduardo Monari	Fraunhofer
Keni Bernardin	Videmo
Kai Nickel	Videmo
Ihar Kliashchou	Regula
Bernhard Strobl	AIT

Contents

- 1. Introduction..... 3
 - 1.1 Scope of the document 3
 - 1.2 Contents of the document 3
 - 1.3 Changes in the European data protection framework..... 3
- 2. Personal data used in MobilePass..... 5
- 3. MobilePass data handling guidelines for R&D activities 7
 - 3.1 Structure of responsibilities 7
 - 3.2 Data protection principles..... 7
 - 3.3 Procedures for collecting and using different types of datasets..... 9
 - 3.4 MobilePass informed consent procedure 10
- Annexes 11
 - A) MobilePass Biometric and Passport Data Collection Consent Form 11
 - B) General legal framework..... 14
 - European Data Protection Framework..... 14
 - The Article 29 Data Protection Working Party 15
 - OECD Privacy Principles..... 17
 - EU FP7 Guidance Notes 18
- Glossary 19
- References..... 20

1. Introduction

This document contains the data handling guidelines for research and testing activities in the Research & Development work packages in MobilePass (WP 3, 4 and 5). MobilePass has received funding from the European Union's Seventh Framework Programme (FP7) for research, technological development and demonstration. Compliance with EU rules on data protection and privacy issues is compulsory for FP7 research projects.

The aim of MobilePass is to develop a mobile system for reliable and quick travel document and identity verification for travellers that consists of a passport reader and biometric verification system. MobilePass research and development in WP 3, 4, and 5 will involve the collecting and processing of biometric and passport data for development and testing purposes. **These biometric and passport data are considered personal data** in the definition of Directive 95/46/EC¹, and their processing is therefore **subject to European rules on data protection and privacy** (art 29 WP 192). This document provides guidelines to the MobilePass technical partners in order to make their R&D activities compliant with all relevant data protection and privacy legislation governing data processing activities.

1.1 Scope of the document

This document contains guidelines for handling data in the research and test activities in WP 3, 4, and 5 in month 1-20. In this phase, research and testing is done under laboratory conditions and may involve human subjects as test persons. These test persons are recruited among MobilePass project personnel and/or other personnel and students of MobilePass partners. The data handling guidelines also provide a basis for handling data during the system integration phase (WP 6), but need to be adapted to the specific data processing activities that will take place in that work package. **The data handling guidelines in this document do not apply to the demonstration phase in WP 7 in month 20-30**, in which the integrated system will be tested at border control points in Romania and Spain, involving real travellers and border guards. For the demonstration phase, separate guidelines will be produced as part of WP2.

1.2 Contents of the document

Section 2 –personal data in MobilePass- gives an overview of the types of personal data that are used in Mobile Pass and of the different R&D activities for which these personal data are processed. In Section 3, the specific data handling guidelines for MobilePass are outlined. These include the description of a structure of responsibilities for data protection within MobilePass and detailed information on the procedures implemented for data protection, data minimisation, and data limitation in the different work packages. Section 3 also includes detailed information on the procedures that will be used for the recruitment of human volunteers. The Annexes include a sample informed consent form and an overview of the (relevant parts of) the European data protection framework.

1.3 Changes in the European data protection framework

The European data protection framework will be changed within the lifetime of the project. The consortium is committed to comply with the new privacy and data protection regulation. It will monitor

¹ 'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is 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' (Directive 95/46/EC)

the changes, and, when necessary, will update the current data handling guidelines document. One of the proposed changes is the introduction of a data protection impact assessment.

Data protection impact assessment

Under article 33 of the proposed regulation, a data protection impact assessment (DPIA) will be required for processing operations that include biometric data. This is independent of the purpose of the processing, hence it also applies to the processing of biometric data for scientific purposes. Such a DPIA would have to contain at least 'a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with [the] Regulation' (Art 33(3)) The assessment should be made available, on request, to the supervisory authority (the national data protection agency). The current deliverable 1.2 already provides a good basis for writing such an assessment.

2. Personal data used in MobilePass

In the R&D work packages in MobilePass (WP 3, 4, and 5 in month 1-20), datasets are collected for developing, testing and evaluating sensor devices and human recognition algorithms in fingerprint and face modalities. In addition, real electronic travel documents may be used for developing and testing the passport reader and for testing biometric verification. MobilePass researchers need to collect biometric features from a limited number of subjects, recorded in the desired mode, and annotated with relevant information about the subject and recording conditions. This involves collecting biometric features from the same subjects for a certain period of time and under different ambient conditions. Samples may also be verified with templates stored on (fake copies of) the electronic travel documents of the subject. MobilePass is a multi-partner research project, and in WP 3, 4, and 5 personal data for testing are expected to be shared among, and modified by different project partners.

In MobilePass WP 3, 4 and 5 the following data processing activities take place, which may include the processing of personal data:

WP number	WP leader	task	Data processing activities	period
3	Regula	3.4	Passport reader test	M12-M28
4	UC3M	4.1	Acquiring fingerprint images (AIT)	M05-M14
		4.2	Optimising of images (FhG)	M08-M24
		4.3	Interoperable feature extraction and comparison (UC3M)	M12-M26
		4.4	Evaluation of the fingerprint recognition subsystem (UC3M)	M18-M28
5	Videmo	5.1	Reference Implementations and Evaluation Dataset (FhG)	M04-M12
		5.4	Evaluation of Face Verification Algorithms (Videmo)	M17-M28

Table 1 Work Package tasks that (may) include testing/research activities in which personal data is used.

WP3: Mobile Computing Platform & Passport Reader

The main objective WP 3 is to create a prototype of a device that is able to perform traveller authentication and background checks. This device may process biographical passport data, and in case of ePassports also digital facial images and fingerprints. For tests in WP 3, a document templates database will be used for document type identification, but this database does not contain personal data. WP 3 also does not need to process personal data for testing. The reader may however be used in WP 4 and 5 to read alphanumeric and/or biometric data from the RFID chip and/or MRZ zones in the passports of test persons. In this context personal data may be transferred among project partners Regula in Daugavpils (Latvia), Videmo and Fraunhofer in Karlsruhe (Germany), and UC3M in Madrid (Spain).

WP 4: Fingerprint Acquisition and Biometric Recognition

The objective of WP 4 is to develop new techniques for identifying individuals based on the touchless acquisition of their fingerprints. The personal data that are processed are fingerprint images (samples and features), and additional data about the human subjects that may influence biometric performance (age, gender, laterality, skin diseases).

In WP 4 the following databases will be used:

- NIST databases
 - Special Database 4 - NIST 8-bit Gray Scale Images of Fingerprint Image Groups.
 - Special Database 27 - Fingerprint Minutiae from Latent and Matching Tenprint Images.
 - Special Database 29 - Plain and Rolled Images from Paired Fingerprint Cards.
- BioSecure
- CASIA Fingerprint Image Database Version 5.0
- FVC2006
- MCYT

In addition to these existing databases, in WP 4 a new dataset for development and testing will be recorded containing “touchless” fingerprints. These fingerprints will be recorded with the acquisition system that is developed as part of task 4.1. The acquisition of the dataset will involve the use of human subjects as volunteers. These volunteers will be recruited among employees and students of the MobilePass partners. In the acquisition and use of this dataset, personal data will be processed by and transferred among the project partners AIT in Vienna (Austria), Fraunhofer in Karlsruhe (Germany) and UC3M in Madrid (Spain).

WP 5: Cooperative Face Verification Development

The objective of WP 5 is to develop new techniques for identifying individuals based on video images of their faces. The personal data that are processed are facial images (sample and features), which consist of both still images and videos.

The following existing database will be used:

- NIST Face Recognition Grand Challenge (FRGC)
- NIST Face and Ocular Challenge Series (FOCS)
- NIST Facial Recognition Technology Database (FERET)
- Labeled Faces in the Wild database (LFW)
- NIST Multiple Biometric Grand Challenge (MBGC)

In addition to these existing databases, in WP 5 a new dataset for development and testing will be recorded. This dataset will contain short videos of subject’s faces and upper body parts. These clips will be recorded with the camera hardware and setup as specified during the MobilePass project. The dataset is needed for algorithm development on data which is in line with later camera specifications.

The acquisition of the dataset will involve the use of human subjects as volunteers. These volunteers will be recruited among employees and students of the MobilePass partners. In the acquisition and use of this dataset, personal data will be transferred among the project partners Videmo and Fraunhofer in Karlsruhe (Germany).

3. MobilePass data handling guidelines for R&D activities

3.1 Structure of responsibilities

Under Directive 95/46/EC the data controller is responsible for compliance with data protection rules. In MobilePass the data controller is the MobilePass consortium. For the development, testing, and evaluation activities in MobilePass, the WP leader under whose responsibility a specific data processing activity takes place represents the data controller and hence is responsible for compliance with data protection rules.

For each R&D work package (WP 3, 4 and 5), a named data controller in the person of the WP leader will be responsible for data management:

WP 3: Ihar Kliashchou (Regula)

WP 4: Belen Fernandez-Saavedra (UC3M)

WP 5: Keni Bernardin (Videmo)

More specifically the WP leader as data controller:

1. Sees to it that all research activities within his/her WP (including those of WP partners) are compliant with the data handling guidelines as detailed in the current document.
2. Provides brief descriptive information [in the Test Plans/Activity Reports] about the datasets that are used for development and testing of technologies (e.g. name of the database, type of data)
3. Provides brief descriptive information [in the Test Plans/Activity Reports] on the recruitment procedure for human volunteers participating in the research.
4. Provides detailed written information on the procedures that will be implemented for data protection (secure storage, access and transfer of data), privacy and confidentiality (in the Data handling guidelines)].
5. Sees to it that each human volunteer (data subject) who participates in the research signs an informed consent form, that the forms are signed on behalf of the MobilePass consortium, and that they forms are kept for future demonstration to the European Commission if required.
6. Acts as the contact person towards data subjects when the data subject requests information, or wants to exercise his/her rights
7. Keeps a file of the names of staff authorized to process data (employees who process data, e.g. lab personnel, interns) and ensures that these are familiar with and understand the MobilePass data handling guidelines.

Note: for the signing of the consent forms (point 5), the WP leader may appoint a representative, e.g. the local principle researcher.

All MobilePass personnel who process personal data commit themselves to conducting research in compliance with the MobilePass data handling guidelines and are accountable for their activities during the course of the project

3.2 Data protection principles

The data protection principles listed below apply to all research and development activities in MobilePass in which personal data are processed. *Data processing* consists of any operation or set of operations which is performed on 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' (EC FP7 Data protection and privacy ethical guidelines). The principles below are based on the European Data Protection Directive (95/46/EC), the opinions of the Article 29 Data Protection Working Party on biometric technologies and the FP7 Data protection and privacy ethical guidelines (see Annexes B-D).

- **Legitimacy:** MobilePass only processes personal data if the data subject has unambiguously given his or her (written) consent, or if there is another legal basis to do so.
 - *For all activities involving the processing of personal data, researchers follow the procedures for collecting and using different types of databases (3.3) and the MobilePass informed consent procedure (3.4)*
- **Purpose limitation:** MobilePass will not use personal data collected during the developing, testing and evaluating for any purposes other than those stated in the consent form.
- **Data limitation:** MobilePass will keep and use data only as long as necessary for the purpose of research and technology development. The WP leader ensures that the data, or profiles derived from such data, are permanently deleted after that justified period of time.
- **Data minimisation:** only data strictly relevant for the purposes stated in the consent form are processed.
 - *Additional personal data will only be collected when these are strictly necessary for the purpose of biometric performance testing*
Example:
-Age and gender (indirectly identifying information) are factors that are known to influence biometric performance and hence data on age and gender may be collected (taking into account the other data protection principles such as informed consent).
 - *No additional directly and indirectly identifying data will be processed when this is not strictly necessary.*
Example:
-If in WP 4 and WP 5 the RFID chip is read to generate reference images for biometric verification, only the relevant biometric data will be stored (and not the alphanumerical data such as passport number and name)
- **Data protection:** data are handled in such a manner as to ensure that they are safe from unforeseen, unintended, unwanted or malevolent use.
 - *Personal data will be securely stored. The data is stored on internal file servers in AES-encrypted containers/partitions at the facilities of the WP partners. Access to the data storage is restricted by password protection.*
 - *The biometric data of each test person will be stored by using a random user identifier. Additional indirectly identifying data (e.g. age or gender) will be encoded. The random user identifier shall not contain any identifying information (such as the subject's name or initials). A single user identifier may be used as part of the file name for different files that belong to the same person: e.g. biometric images taken under different conditions and the additional indirectly identifying information of the test person.*

- *Biometric data will be stored according to the principle of functional separation. This means that the biometric information is stored separately from other identifying information:*
 1. *The biometric data of test persons is stored separately from the name or ID number of the test person.*
 2. *The indirectly identifying information (e.g. age, gender) will be encoded and stored separately from the name or ID number of the test person.*
 3. *If two types of biometrics (fingerprint and facial image) are collected from one and the same test person, the fingerprint and facial image² will be stored separately.*
- *The list associating the user identifiers with the names or ID numbers of the test persons shall be encrypted and stored at a separate location (e.g. an USB), with access only on a need-to-know basis.*
- *Only staff who are assigned to the relevant WPs in MobilePass have access to the data.*
- *Transfer of personal data between MobilePass partners will be secured. The following methods are preferred: FTP/HTTP via VPN; SFTP; Download of encrypted archives via HTTP(S); or encrypted partitions on external hard drives.*
- **Rights of data subjects:** data subjects have the right to request access to their personal data, and to correct, if applicable, and delete personal data

3.3 Procedures for collecting and using different types of datasets

In MobilePass, different types of datasets containing personal data may be collected and used. The following procedures apply:

Using existing in-company/public datasets in MobilePass:

In MobilePass, data from a previously gathered set – either by the MobilePass partner or from another project or institute – may be used. When using an existing database that contains personal data, MobilePass researchers will check if the initial informed consent covers this complementary use of the data. If this is not the case, a new informed consent for the study needs to be obtained (see procedure below).

Collecting new datasets from publicly available data in MobilePass:

Before using publicly available data, MobilePass researchers will first check if there is a legal basis for the biometric processing of this data. MobilePass follows the recommendation of the Article 29 Working Party on the use of publicly available data(sets) for biometric processing³ and will not extract

² facial images are directly identifying information and hence should be stored separately from other biometric data and from the name or ID number of the test person.

³ The Article 29 Data Protection Working Party has argued that '[p]hotographs on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose.'

biometric templates from publicly available data when there is no specific legal basis (e.g. consent) for this.

Collecting new datasets with human volunteers in MobilePass:

When collecting new datasets containing personal data of human volunteers (passport data and/or biometric data), MobilePass will seek informed consent prior to data processing (see procedure below).

3.4 MobilePass informed consent procedure

When human subjects are involved as volunteers in MobilePass (e.g. as test persons providing biometrics) **informed consent is required**. In MobilePass, the informed consent procedure entails the recruitment of healthy adult participants who voluntarily participate in the research, and who, prior to participation, are informed about the goals, content, and procedures of the research and give their written approval.

Specific MobilePass recruitment principles:

-Only healthy adult volunteers will be recruited among the personnel and/or students of the MobilePass project partners.

-Subjects unable or less able to give their free and informed consent will be excluded.

-Subjects will not be paid but only reimbursed for the time and expenses devoted to the participation in the research. Reimbursement will be such as to exclude any form of undue inducement.

-The researcher will explain orally the goals, content and procedures of the study, and the subject is required to read and sign an informed consent form in English and the applicable local language.

A sample informed consent form compliant with EC FP7 guidelines is included in this document (Annex A). In case a MobilePass partner prefers to create their own informed consent form, please make sure all EC requirements are fulfilled. For guidelines see

http://ec.europa.eu/research/participants/data/ref/fp7/89807/informed-consent_en.pdf

Annexes

A) MobilePass Biometric and Passport Data Collection Consent Form⁴

Purpose

The.....(*name of the institution/lab which is carrying out the study*)..... is carrying out scientific research on the acquisition and verification of biometric (fingerprint images, face images) and passport data. The overall goal of the study is to develop a handheld biometric device that allows European border control authorities to check travellers in a comfortable, fast, and secure way. The study is part of a larger European research project called MobilePass (full title: A secure, modular and distributed mobile border control solution for European land border crossing points), funded by the European Commission within the scope of the 7th Framework Programme (GA no: 608016). In the current project phase, MobilePass uses human volunteers to acquire datasets for developing, testing and evaluating sensor devices and algorithms for fingerprint and face recognition. In addition, real passports may be used for developing and testing the passport reader and for testing biometric verification.

Procedure

In order to provide training and experimental data necessary to the theoretical and practical research and development activities required by the MobilePass project, a number of physical features will be recorded under different ambient conditions. In the session/sessions you are invited to participate in we will record.....(*give a detailed description of the specific procedure*)

In this session/these sessions we are going to collect the following personal characteristics: (*give a description of the type of data, eg fingerprint/face/personal data and security features from passport (MRZ/RFID etc) Please also mention any additional personal data you may record such as gender, age, etc.*)

Each session will last approximately.....(*give a reasonable estimate*).....and individuals may discontinue their participation at any time for any reason without any need to give an explanation for their wish to stop their participation.

Data protection, confidentiality and privacy

All personal data stored during the study will be completely and irreversibly anonymised (unless this refutes the purpose of the study), or be erased on completion of the MobilePass Project. No personal data will ever be used for any purposes other than those stated in this form. Your personal data will not be transferred to any third party or be commercialised. When your data is stored it will be encrypted and access to the data storage is restricted by password protection. Your personal data may be used by MobilePass project partners located in different European countries. Only staff who are assigned to the relevant WPs in MobilePass have access to the data and transfer of personal data between MobilePass partners will be secured.

The investigator will record the data collected in a file. This file will be identified only by a random user identifier. Your biometric data will be stored separately from other identifying information (such as

⁴ The authors have used the consent form that was developed European research project ACTIBIO as an example for drafting this form (Mordini, Ashton and Massari 2009)

your name or ID number). The link associating the random user identifier with you is stored separately and securely.

The results of the study may be published in scientific books or journals or may be used for didactic purposes. However, no identifying information about you (name, facial photograph) will ever be revealed in any document, publication or teaching materials.

You may exercise your rights of access, rectification and deletion of data at any time. In order to do so, you will need to communicate your wish to do so to[the WP leader]..... by email to the following address

Right to get more information about the study

You can ask any questions about the study at any time throughout the recording period. The investigator will be available to answer to your questions or concerns about the study. You will be informed of any new discovery that could occur throughout the study and that may affect your participation in future studies. If during the study and thereafter you wish to discuss your rights as a person who participates in an investigation, your participation in the study or your concerns about it, or if you do not want to continue in that investigation or future research, please contact[the WP leader] any time you wish.

Refusal or cessation of participation

Your participation in this study is voluntary. You do not have to participate in the study if you do not want to do so. If you choose to participate, you can change your mind or leave the study at any time without having to give explanations and without being affected in any way by this decision. Similarly, at the discretion of the investigator, you may be withdrawn from the study for any of the following reasons: (a) if the minimum requirements of the study are not met (b) if for any reason the study is interrupted.

Risks and discomforts

The personal risk by participating in this study does not exceed the risks of daily and normal life. None of the procedures represent a danger to your health or to physical and mental integrity.

Financial Compensation

You understand that there is no financial compensation for participating in this study, but you may be reimbursed for the working hours lost due to participation, or other costs incurred because of your participation (e.g. travel costs).

Consent

By signing the present form, I, the undersigned, understand and consent freely that my personal data, including biometric data, my name and contact details, will be collected and processed by[the lab/institute]....., the data controller, and by appointed processors on behalf of the data controller, in accordance with applicable laws and with what is stated in the present clause. I have been informed about the study carried out within the scope of the MobilePass project and its purposes have been explained to me.

I understand that my personal data will be encoded in order to safeguard confidentiality, and that if results of the study are published, my identity will not be revealed. I also understand that I have the right to request access to my personal data, to correct, if applicable, and delete my personal data in

conformity with the applicable legislation. For these purposes, I can contact[WP leader].....

I have read the above and I understand that I can refuse to participate in this study without any direct or indirect negative consequence on my life.

By signing the present form, I agree with the above.

[the volunteer]

Date: _____ Place:

Name:

Signature:

Email:

Telephone:

The undersigned responsible declares to have explained the purpose of the investigation, the procedures used in the study, and any potential risks and inconvenience that are likely to arise from participation. They have responded to the best of their abilities to the questions asked with respect to the study.

[the investigator]

Date: _____ Place:

Name:

Signature:

B) General legal framework

European Data Protection Framework

Directive 95/46/EC is the main legal framework for the processing of personal data within the European Union.

Relevant provisions of Directive 95/46/EC (1995)

Principles relating to data quality (Article 6): personal data must be:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- (e) 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.

The responsible entity is the data controller (art. 6^o2, 16, 17, 18, 19). There has to be a responsible controller to ensure data protection rights and duties. For the purpose of article 6.1, the responsible entity is the data controller (6.2)

Criteria for making data processing legitimate (Article 7): personal data may be processed only if the data subject has unambiguously given his consent (7a)

Information to be given to the data subject (Article 10-11). The data subject has a right to know about the processing and the use of the processed data.

The data subject's right of access to data (Article 12): The principle is that all data subjects are endowed with a right of access to the biometrical data and to obtain rectification, erasure or blocking of data when the processing violates the provisions (e.g. incomplete or inaccurate nature of the data).

Confidentiality of processing (Article 16): 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, unless he is required to do so by law.

Security of processing (Article 17): 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.

Obligation to notify the supervisory authority (art.18) Before processing any personal data the supervisory body has to be notified of the purposes of the processing;

The Article 29 Data Protection Working Party

The Article 29 Data Protection Working Party is an independent European advisory body and was set up under the Directive 95/46/EC. It has advisory status and acts independently.

In 2012, the Working Party adopted Opinion 3/2012 on developments in biometric technologies. In this Opinion, the Working Party states that 'biometric data are in most cases personal data. Therefore they may only be processed if there is a legal basis and the processing is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'.

The Working Party calls attention to the principle of purpose limitation, proportionality, necessity and data minimisation principles in particular.

Purpose: A prerequisite to using biometrics is a clear definition of the purpose for which the biometric data are collected and processed, taking into account the risks for the protection of fundamental rights and freedoms of individuals.

Proportionality: The use of biometrics raises the issue of proportionality of each category of processed data in the light of the purpose for which the data are processed. As biometric data may only be used if adequate, relevant and not excessive, it implies a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way.

Accurate: Biometric data processed must be accurate and relevant in proportion to the purpose for which they were collected.

Data minimisation: A specific difficulty may arise as biometric data often contain more information than necessary for matching functions. The principle of data minimisation has to be enforced by the data controller. Firstly, this means that only the required information and not all available information should be processed, transmitted or stored. Second, the data controller should ensure that the default configuration promotes data protection, without having to enforce it.

Retention period: The controller should determine a retention period for biometric data that should not be longer than is necessary for the purposes for which the data were collected or for which they are further processed. The controller must ensure that the data, or profiles derived from such data, are permanently deleted after that justified period of time.

3.1 Legitimate ground

The processing of biometric data must be based on one of the grounds of legitimacy provided for in Article 7 of Directive 95/46/EC. The first such ground of legitimacy given in Article 7(a) is where the data subject has given consent to the processing.

According to the Data Protection Directive, Article 2(h), consent must be freely given, specific and represent an informed indication of the data subject's wishes.

Furthermore, consent must be revocable. In this regard, in its opinion on the definition of consent, the Working Party underlines various important aspects of the notion: the validity of consent; the right of individuals to withdraw their consent; consent given before the beginning of the processing; requirements regarding the quality and the accessibility of the information.

Consent is only valid when sufficient information on the use of biometric data is given. Since biometric data may be used as a unique and universal identifier providing clear and easily accessible information

on how the specific data are used is to be regarded as absolutely necessary to guarantee fair processing. Therefore this is a crucial requirement for a valid consent in the use of biometric data.

3.4. Transparency and information of the data subject

According to the principle of fair processing, data subjects must be aware of the collection and/or use of their biometric data (Art. 6 of Directive 95/46/EC). Any system that would collect such data without the data subjects' knowledge must be avoided. The data controller must make sure that data subjects are adequately informed about the key elements of the processing in conformity with Article 10 of the data protection directive, such as their identity as controller, the purposes of the processing, the type of data, the duration of the processing, the rights of data subjects to access, rectify or cancel their data and the right to withdraw consent and information about the recipients or categories of recipients to whom the data are disclosed. As the controller of a biometrics system is obliged to inform the data subject, biometrics must not be taken from somebody without his knowledge.

3.5. Right to access biometric data

Data subjects have a right to obtain from the data controllers access to their data, in general including their biometric data. Data subjects also have a right to access possible profiles based on these biometric data. If the data controller has to ascertain the identity of the data subjects to grant this access, it is essential that such access is provided without processing additional personal data.

3.6. Data security

The data controllers must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. Any data collected and stored must be appropriately secured.

3.8. Sensitive data

Some biometric data could be considered sensitive in the meaning of Article 8 of Directive 95/46/EC and in particular, data revealing racial or ethnic origin or data concerning health. For example DNA data of a person often include health data or can reveal the racial or ethnic origin. In this case DNA data are sensitive data and the special safeguards provided by article 8 must apply in addition to the general data protection principles of the Directive. In order to assess the sensitivity of data processed by a biometric system the context of the processing should also be taken into account.

OECD Privacy Principles

The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (“1980 Guidelines”) contain the first internationally agreed-upon set of privacy principles:

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

Individuals should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
- b) to have communicated to them, data relating to them
 - i. within a reasonable time;
 - ii. at a charge, if any, that is not excessive;
 - iii. in a reasonable manner; and
 - iv. in a form that is readily intelligible to them;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

EU FP7 Guidance Notes

Informed consent: http://ec.europa.eu/research/participants/data/ref/fp7/89807/informed-consent_en.pdf

Data protection and privacy ethical guidelines:

http://ec.europa.eu/research/participants/data/ref/fp7/89827/privacy_en.pdf

Glossary

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

Data processor: a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf.

Data protection: data protection consists of a framework of security measures designed to guarantee that data are handled in such a manner as to ensure that they are safe from unforeseen, unintended, unwanted or malevolent use.

Directly identifiable personal data: consist of information that identifies a specific individual through direct identifiers (e.g., name, passport number, national ID card number).

Indirectly identifiable personal data: consists of background information such as place of residence or institutional affiliation, combined with data on age, gender, occupation, diagnosis, etc.

Personal data: consist of information relating to an identified or identifiable person ('data Subject' or research participant); An identifiable person is 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 appearance, physiological, mental, economic, cultural or social identity;

Processing of personal data: ('processing') consists of any operation or set of operations which is performed on 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.

References

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, OJ L 281, 23.11.1995. Retrieved from <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en>

European Commission (2012). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. COM(2012) 11 final. Retrieved from <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en>

European Commission (2009), *Ethical review in FP7, data protection and privacy ethical guidelines*. Retrieved from http://ec.europa.eu/research/participants/data/ref/fp7/89827/privacy_en.pdf

European Commission, *Ethical review in FP7, guidance for applicants: informed consent*. Retrieved from http://ec.europa.eu/research/participants/data/ref/fp7/89807/informed-consent_en.pdf

Mordini, E., H. Ashton, and S. Massari (2009) *ACTIBIO Ethical Manual* (ACTIBIO D8.1). Retrieved from ACTIBIO website: http://www.actibio.eu/actibio/files/document/Deliverables/ACTIBIO_Deliverable_8.1.pdf

OECD Organisation for Economic Co-operation and Development (2013) *Guidelines governing the protection of privacy and transborder flows of personal data*. C(80)58/FINAL. Retrieved from <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>

WP29 (Article 29 Working Party) (2012) *Opinion 3/2012 on developments in biometric technologies*, 27 April 2012.

WP29 (Article 29 Working Party) (2003) *Working document on biometrics*, 1 August 2003