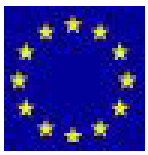
PrivAcy pReserving Infrastructure for Surveillance

Deliverable D2.4
Guidelines for SALT Conceptual Frameworks v2

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D2.4
Title:	Guidelines for SALT Conceptual Frameworks v2
Version:	v1.0
Date:	31/12/2015
Confidentiality:	Public
Editor:	Claire Gayrel (CRIDS-UNamur)
Contributors:	Claire Gayrel (CRIDS-UNamur) Fanny Coudert, Lina Jasmontaite, Stephanie Mihail (KU Leuven) Daniel Le Métayer (INRIA) Antonio Kung, Christophe Jouvray (Trialog)



Funded by the European Union's Seventh Framework Programme

Table of Contents

DOCUMENT HISTORY

Version	Status	Date
V0.1	Liminal draft Unamur	01/10/2015
V0.2	Second draft Unamur	15/11/2015
V0.3	INRIA and KUL contribution	07/12/2015
V0.4	Edition of a final draft	11/12/2015
V1.0	Final draft submitted	31/12/2015

Approval		
	Name	**Date**
Prepared	Claire Gayrel, Fanny Coudert, Daniel Le Metayer	01/10/2015
Reviewed	Antonio Kung	
Authorised	Antonio Kung	

Circulation	
Recipient	**Date of submission**
Project partners	11/12/2015
European Commission	31/12/2015

Executive Summary

The mission of PARIS is to define and demonstrate a methodological approach for the development of surveillance infrastructure, which enforces the right of citizens for privacy, justice and freedom. To do that, we attempt to build a SALT (Socio-ethicAl, Legal and Technical) framework which is both theoretical and methodological, and which encompasses various dimensions. First, SALT frameworks are knowledge-based and need data collection. Second, this knowledge must be analyzed and represented so that it can be included in a smart digital representation. Third, these representations are built in a repository which contains all the relevant knowledge for SALT framework and which can evolve over time with the management capability. Fourth and lastly, this knowledge can be processed and applied to specific systems by systems designers.

D.2.1 described the “Concepts and Contexts” to help the characterization and definition of the main relevant criteria - regards to the relationships between privacy and surveillance - which have to be considered in the definition of the SALT framework, while taking into account socio-contextual, ethical, legal, and technical privacy’s dimensions and the concept of accountability. It achieved a well-documented overview of the current European landscape recorded about the relationship between privacy and surveillance, using cutting-edge scientific literature, laws, institutional and policy documents, and studies funded by the European Commission.

D.2.2 dealt with the “structure and dynamics of SALT framework”. It showed that a SALT framework is defined as a collection of concepts and overarching principles concerning privacy

in public spaces that will be used as a reference for the design of surveillance systems. Such principles integrate a variety of perspectives on this issue, namely Socio-contextual and ethicAl, Legal, and Technical. In addition, it demonstrated that a SALT framework offers a framework management capability, which means that a SALT framework can evolve over time, broaden its knowledge-base and that it is flexible so as to include new inputs from SALT experts.

D2.3. relied upon key findings from D2.1 and D2.2 and targeted SALT users, i.e. the people in charge of applying the SALT frameworks. It provided tentative guidelines for future users of SALT framework. Mostly, it addressed SALT system designers and SALT system owners. Guidelines are defined as methodological tools aimed at facilitating the application of the SALT frameworks, through the appropriate use of SALT references and the application of SALT processes. In this respect, it fits within the framework of WP2 that aims to define and make operative the concepts of SALT framework.

The present deliverable D2.4 is an update of the D2.3 Guidelines. The introduction explains how the deliverable has been framed, what are its purposes and what it intends to realize, i.e. facilitating the appropriation and use of SALT frameworks by SALT users. To do that, it first grounds the “Guidelines for users” in a “domain approach” (1.2) and explain the main inputs and outputs of the guidelines for users (1.2), assuming that the most relevant entry point to SALT framework depends upon the user’s desired level of expertise.

The section 2, “Concepts of SALT frameworks for users” introduces the main concepts used in the SALT framework in an easy and understandable way, so that SALT users may easily apprehend what SALT frameworks are about, what they deal with and what they encompass. It starts by introducing the approach decided upon in D2.2., namely a questionnaire-based approach to cope with legal, socio-contextual and ethical, technical and accountability dimensions (2.1). Then it recalls the three-stage process, i.e. that SALT systems are put into place sequentially. In this respect, we identified three stages of development of a surveillance system: conception, design and implementation (2.2). Lastly, it introduces the guidelines and their definition, their purpose, and the extent to which they will be useful for SALT users (2.3).

Section 3 & 4 are dedicated to the guidelines for users of SALT frameworks. Section 3 presents the guidelines for creators of references, namely the SALT experts. Although PARIS partners have agreed about a common template (3.1), specific guidelines are addressed for each category of references, namely for socio-ethical and contextual references (3.2), legal references (3.3), and technical references (3.4).

Section 4 introduces the guidelines domain by domain. First, it deals with the socio-contextual and ethical dimensions, and suggests a certain amount of guiding principles for applying SALT frameworks under these dimensions (4.1). Second, it addresses the legal dimensions of SALT processes and explains how to integrate certain fundamental legal notions such as privacy, data protection, or yet the principle of proportionality among others (4.2). Third, it deals with the technical dimensions and identifies the relevant technical users and provides step-by-step guidelines that will take him/her through the development process (4.3). Lastly, we examine the accountability dimension (4.4). This dimension crosscuts many aspects of both the socio-contextual and ethical, legal and technical dimensions.

In addition to the “Guidelines for users”, this report also contains five annexes, gathering all the contributions prepared by the main partners involved in the definition of a SALT framework in relation to biometric systems. Indeed, as suggested in D2.1 and D2.2, a specific research has been carried out in order to prepare a SALT questionnaire for biometric systems of authentication. The SALT biometric questionnaire aims at providing appropriate assistance to

decision-makers regarding the conception, design and implementation of a biometric system. Altogether, these five annexes summarizes the research carried out during the last period of PARIS project and constitute a concrete illustration of the application of the concepts described in section 2 and the guidelines and principles explained in section 4 of the deliverable.

More specifically, Annex 1 constitutes an introduction to the biometric questionnaire and explains the methodology applied for the selection of the criteria to be taken into account in order to assess the proportionality of a biometric system in a first stage. This research has included an extensive study of the French caselaw in relation to biometric systems, contributions from the Council of Europe, the Working Party 29 and literature. Annex 2 contains the final draft of the biometric questionnaire aiming at assessing the "opportunity" of a biometric system in the light of the criteria of purpose, legitimacy and necessity. Annex 3 is dedicated to the issue of consultation of stakeholders and how such consultation is included in the SALT questionnaire through questions and specific recommendations according to the categories of people enrolled in the system. Annex 4 deals with the "Design" phase and includes all the questions that should be addressed step-by-step by systems designers and system owners when designing a biometric system. Annex 5 relates to the third phase of the questionnaire "final balancing" and Annex 6 deals with the issue of governance, providing guidelines to draft an internal privacy policy for the management of the biometric system installed.

List of Figures

List of Tables

Abbreviations and definition

Abbreviation	Definition
Article 29 WP	Article 29 Data Protection Working Party
CCTV	Closed Circuit Television
CNIL	Commission Nationale Informatique et Libertés (FR)
COE108	Council of Europe Convention 108
DPIA	Data Protection Impact Assessment
ECHR	European Court (or Convention) of Human Rights
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EC	European Community
EGE	European Group on Ethics in Science and New Technologies
EU	European Union
FIPS	Fair Information principles
IA	Impact Assessment
ICT	Information and Communication Technologies
JO	Journal Officiel (FR)
MB	Moniteur Belge (BE)
OECD	Organization for Economic Co-operation and Development
OJEC	Official Journal of the European Community
OJEU	Official Journal of the European Union
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PET	Privacy-Enhancing Technologies
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification
RTP	Real Time Transport
SALT	Social, ethicAl, Legal, Technical
WP	Working Paper

1 Introduction

1.1 Deliverable objective and scope

The mission of PARIS is to define and demonstrate a methodological approach for the development of surveillance infrastructure, which enforces the right of citizens for privacy, justice and freedom. To do that, we attempt to build a SALT (Socio-ethicAl, Legal and Technical) framework which is both theoretical and methodological, and which encompasses various dimensions. First, SALT frameworks are knowledge-based and need data collection. Second, this knowledge must be analyzed and represented so that it can be included in a smart digital representation. Third, these representations are built in a repository which contains all the relevant knowledge for SALT framework and which can evolve over time with the management capability. Fourth and lastly, this knowledge can be processed and applied to specific systems by systems designers.

D.2.1 described the "Concepts and Contexts" to help the characterization and definition of the main relevant criteria - regards to the relationships between privacy and surveillance - which have to be considered in the making of the SALT framework, while taking into account socio-contextual, ethical, legal, and technical privacy's dimensions and the concept of accountability. It achieved a well-documented overview of the current European landscape recorded about the relationship between privacy and surveillance, using cutting-edge scientific literature, laws, institutional and policy documents, and studies funded by the European Commission.

D.2.2 dealt with the "structure and dynamics of SALT framework". It showed that a SALT framework is defined as a collection of concepts and overarching principles concerning privacy in public spaces that will be used as a reference for the design of surveillance systems. Such principles integrate a variety of perspectives on this issue, namely Socio-contextual and ethicAl, Legal, and Technical. In addition, it demonstrated that a SALT framework offers a framework management capability, which means that a SALT framework can evolve over time, broaden its knowledge-base and is flexible so as to include new inputs from SALT experts.

D2.3. relied upon key findings from D2.1 and D2.2 and targeted SALT users, i.e. the people in charge of applying the SALT frameworks. It provided tentative guidelines for future users of SALT framework. Mostly, it addressed SALT system designers and SALT system owners. Guidelines are defined as methodological tools aimed at facilitating the application of the SALT frameworks, through the appropriate use of SALT references and the application of SALT processes. In this respect, it fits within the framework of WP2 that aims to define and make operative the concepts of SALT framework.

The present deliverable D2.4 is an update of the D2.3 Guidelines. This introduction explains how the deliverable has been framed, what are its purposes and what it intends to realize, i.e. facilitating the appropriation and use of SALT frameworks by SALT users. To do that, it first grounds the "Guidelines for users" in a "domain approach" (1.2) and explain the main inputs and outputs of the guidelines for users (1.2), assuming that the most relevant entry point to SALT framework depends upon the user's desired level of expertise.

The section 2, "Concepts of SALT frameworks for users" introduces the main concepts used in the SALT framework in an easy and understandable way, so that SALT users may easily apprehend what SALT frameworks are about, what they deal with and what they encompass. It starts by introducing the approach decided upon in D2.2., namely a questionnaire-based approach to cope with legal, socio-contextual and ethical, technical and accountability

dimensions (2.1). Then it recalls the three-stage process, i.e. that SALT systems are put into place sequentially. In this respect, we identified three stages of development of a surveillance system: conception, design and implementation (2.2). Lastly, it introduces the guidelines and their definition, their purpose, and the extent to which they will be useful for SALT users (2.3).

Section 3 & 4 are dedicated to the guidelines for users of SALT frameworks. Section 3 presents the guidelines for creators of references, namely the SALT experts. Although PARIS partners have agreed about a common template (3.1), specific guidelines are addressed for each category of references, namely for socio-ethical and contextual references (3.2), legal references (3.3), and technical references (3.4).

Section 4 introduces the guidelines domain by domain. First, it deals with the socio-contextual and ethical dimensions, and suggests a certain amount of guiding principles for applying SALT frameworks under these dimensions (4.1). Second, it addresses the legal dimensions of SALT processes and explains how to integrate certain fundamental legal notions such as privacy, data protection, or yet the principle of proportionality among others (4.2). Third, it deals with the technical dimensions and identifies the relevant technical users and provides step-by-step guidelines that will take him/her through the development process (4.3). Lastly, we examine the accountability dimension (4.4). This dimension crosscuts many aspects of both the socio-contextual and ethical, legal and technical dimensions.

In addition to the “Guidelines for users”, this report also contains five annexes, gathering all the contributions prepared by the main partners involved in the definition of a SALT framework in relation to biometric systems. Indeed, as suggested in D2.1 and D2.2, a specific research has been carried out in order to prepare a SALT questionnaire for biometric systems of authentication. The SALT biometric questionnaire aims at providing appropriate assistance to decision-makers regarding the conception, design and implementation of a biometric system. Altogether, these five annexes summarizes the research carried out and constitute a SALT conceptual framework for biometrics and a concrete illustration of the application of the concepts described in section 2 and the guidelines and principles explained in section 4 of the deliverable.

Annex 1 constitutes an introduction to the biometric questionnaire and explains the methodology applied for the selection of legal criteria. This research has included an extensive study of the French caselaw in relation to biometric systems, contributions from the Council of Europe, the Working Party 29 and literature. Annex 2 is dedicated to the first phase of the biometric questionnaire aiming at assessing the “opportunity” of a biometric system in the light of the criteria of purpose, legitimacy and necessity of a biometric system. Annex 3 is dedicated to the consultation of stakeholders and how such consultation is included in the SALT questionnaire through both questions and specific recommendations according to the categories of people enrolled in the system. Annex 4 deals with the “Design” phase and includes all the questions that should be addressed step-by-step by systems designers and system owners when designing a biometric system. Annex 5 relates to the third phase of the questionnaire “final balancing” and Annex 6 deals with the issue of governance, providing guidelines to draft an internal privacy policy for the management of the biometric system installed.

1.2 A domain approach

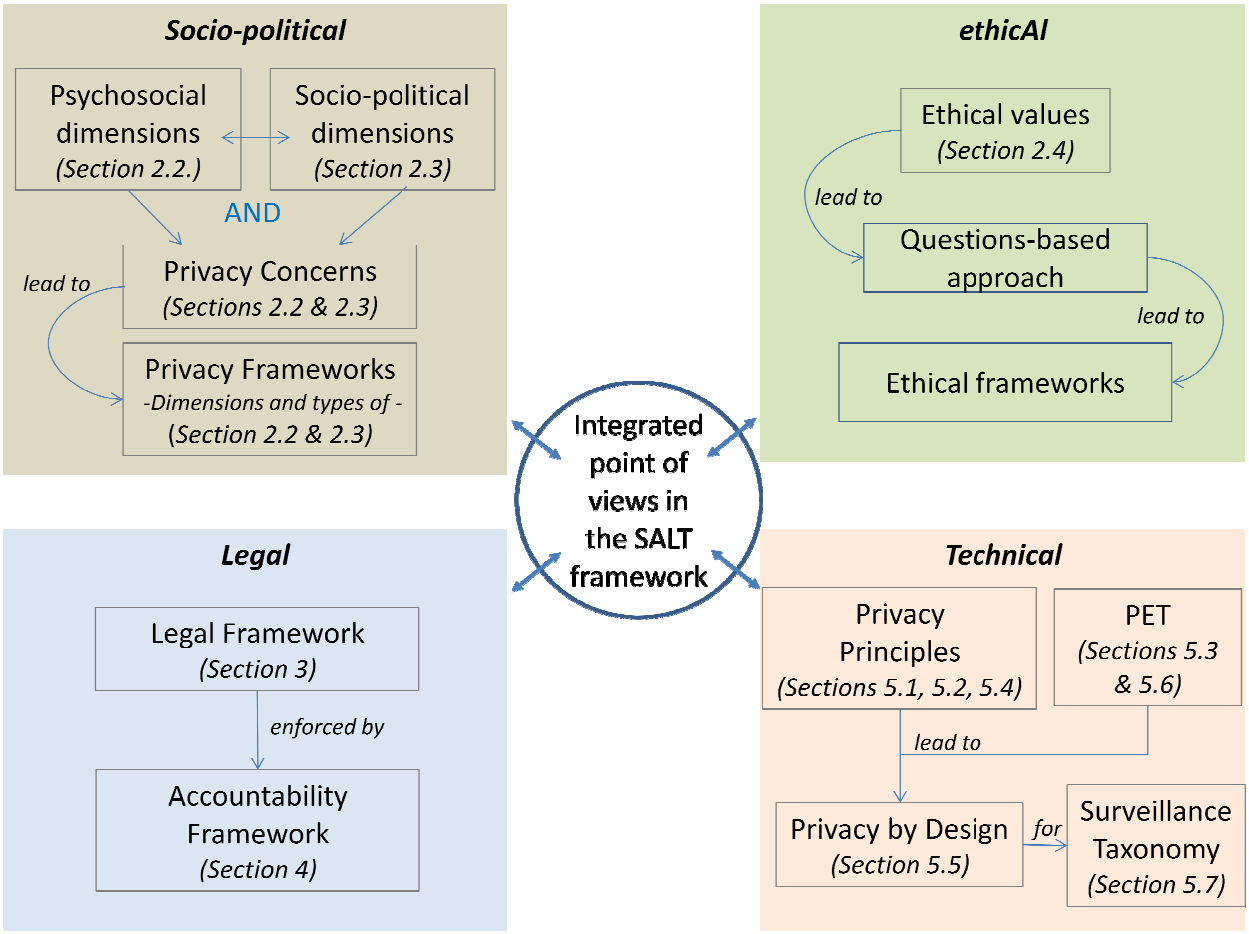


Figure 1 Integrating dimensions for a domain approach

SALT frameworks are interdisciplinary in scope. They encompass a wide variety of perspectives and put experts from different disciplines together, e.g. lawyers, ethicist, engineers, … On the other side, the same is true for the SALT users, which cannot be expert is all these fields at once. So in PARIS we attempt at overcoming the classical division of labor resulting from disciplinary boundaries. We define a comprehensive one-size-fits-all tool which encompasses all the dimensions at once, so as to overcome such limitations.

This approach is both very demanding and very challenging. It is not easy for experts from different disciplines to come together and design a unique SALT framework that could apply and be used with respect to a variety of surveillance systems. To give one example, in D2.2., we reflected on the complex dynamics of learning which occurred between computer scientists and legal experts. More specifically, this learning occurred in the challenge of learning how to integrate in a digital manner the legal requirements, that vary from one Member State to the other and requires interpretation in very specific situations. In this respect, the PARIS project was very challenging and this challenge has been taken very seriously.

How does that reflect upon the users guidelines in this deliverable? We decided to go for a domain approach, which we deem to be most relevant for users. So that they will be able to get in the system through their area of expertise, either if they come more from the socio-contextual and ethical sides, or from the legal sides, or from technical and accountability sides.

Whatsoever, this main access will be usefully complemented by the other domain. If a user comes from one of the domain, he will still have fruitful entries in all the other different dimensions. Accordingly, users enter by domain in the framework and will be guided through it according to their expertise and needs.

It is important to recall that, in our interdisciplinary perspective, what matters most in terms of achievement while using SALT frameworks is precisely the circle described in Figure 1, which rests at the middle of the four mentioned domains. This means that SALT frameworks succeed when the user, whatever his main domain, i.e. entry point to the SALT framework, manage to take into considerations all of the other relevant dimensions in an integrative manner. Since the use of the SALT framework is not compulsory, but voluntary, its use nevertheless depends on the will of the users to take the exercise seriously.

1.3 Inputs and outputs of guidelines

Guidelines are made for SALT users and SALT owners mainly (as defined in D4.1 and D4.2), but this depends on each kind of targeted domain. In section 3, we address guidelines to SALT experts when they create/introduce new references. In section 4 the guidelines described are rather addressed to the systems owners and system designers and detail which kind of users are targeted by which kind of guidelines, depending on the specifics of each knowledge domains.

The guidelines are methodological tools, which aim at taking the SALT user through the whole process of designing surveillance systems. They facilitate the introduction to SALT concepts and vocabulary, and they render explicit how to use the SALT references throughout the SALT process. The idea is that the process must be convenient for the user who has to be able to get a full grasp on all the other dimensions he/she is not spontaneously familiar with.

In this respect, the inputs that one can expect out of SALT frameworks may seem limited, but are still valuable. They are limited because SALT cannot achieve mechanical compliance, by determining socio-contextual and ethical, legal, technical and accountability “parameters” too rigidly. This means that the responsibility of the output of the system rests on the users, who cannot stay passive and have to be proactive while using the SALT framework, which supports the conception, design and implementation of the surveillance system.

On the other hand, the user receives many inputs for taking into considerations other fields of expertise or other domains than the one he is accustomed to. For instance, the SALT references is beneficial because it provides the SALT user with a massive amount of knowledge which is made easy to access, understand and use. In this respect, the user will take into consideration many dimensions so as to provide a genuine learning process throughout following the SALT process.

In addition, the SALT framework expects its users to provide their own input to the system, according to the output they receive and how satisfying is their experience. In that respect, SALT references are evolving over time with the knowledge of users who become SALT experts. In this way, SALT is a very rewarding system because it facilitates users’ inputs.

The consequence of all this is that the SALT representation goes away from strict legal or ethical compliance, but intends to generate a reflection on socio-contextual and ethical, legal, technical and accountability issues. Compliance thus rests on the process rather than on the result. And so it goes with socio-contextual and ethical issues.

SALT frameworks provide tools to help thinking through these dimensions but do not provide straight answers to the questions it raises by itself. For that, it takes close consideration of the designer of the system and relevant stakeholders, so that these issues can be discussed collectively. The output is henceforth a strong richness of content added to the process, which grants the user with added value through the amount of expertise made available.

This deliverable is intended to help the users to learn how to use SALT frameworks, in order for the users to get practical advice and methodological insights into how SALT frameworks operate, what can be expected out of them, and what they cannot provide.

2 Concepts of SALT Frameworks for users

A SALT framework can be defined as a collection of concepts and overarching principles concerning privacy that will be used as a reference for the design of surveillance systems. Such principles integrate a variety of perspectives on this issue, namely **S**ocio-contextual and ethic**A**l, **L**egal, and **T**echnological.

In addition, a SALT framework offers a framework management capability. SALT frameworks evolve over time, broaden their knowledge-base and are flexible to include new inputs from SALT experts. Thus it is possible to customize and enhance SALT frameworks.

In this section, we explain why the SALT framework rests on a questionnaire-based approach backed up by a wide knowledge-based repository. We explain why this approach is the most relevant for SALT users who are mostly, at this stage, system designers and system owners. Then we explain the three stages process that is the various normal stages of development of a surveillance system. We identify three stages: intention, design, and implementation. While at each stage of development of the process, questions must be answered to and issues must be raised, yet SALT frameworks allow for flexibility and retroaction feedbacks, so that the tool is at the same time sequential and dynamic. In point 2.3 we underline the status of the guidelines which follow in section 3 & 4, and why they facilitate the use of the SALT frameworks and their evolution over time.

2.1 A questionnaire-based approach

In D2.1., we concluded that there were already a great diversity of approaches to ethical dimensions, as well as many operational frameworks. Hence there is no need to totally redesign a tool, but rather to learn from the existing ones and to adjust them to what the SALT framework wishes to achieve. In this perspective, we recommended to focus on David Wright's proposition for frameworks for privacy and ethical impact assessment (PIA and EIA). D2.1. also highlighted the potential of a questionnaire approach in its recommendations. This approach implies also a challenge for the design of the SALT framework while fostering stakeholder's thinking and decision, rather than offering them predefined answers.

In D2.2., we presented a range of tools targeted to the decision-maker, that is the person who makes a decision regarding a system. In the case of SALT systems, it can be many persons and stakeholders: system designer or system owner mostly, but at different levels it can also be system users or relevant civil society organizations. In D2.2. we suggested a typology and sorting of all the different actors and their roles. Many tools allow for broadening the scope of the decision to relevant stakeholders (or the general public depending on who is targeted by the system), which is what the SALT also wants to achieve.

One of the key challenges for the SALT framework is to integrate the questions-based approach chosen by Wright and to address privacy issues (including ethical issues) in such a way that those questions will be likely to generate self questioning for the user of the SALT framework and eventually debate among stakeholders. In the case of the SALT framework it appears that the checklist of questions, hence the ethical questionnaire, is the most appropriate tool, since the SALT framework targets mostly system designers at an applied stage of development.

This is why we opted for a « ask questions » approach, hence a questionnaire (Wright, p. 200). Such an approach is rather commonplace and heavily relies on European Commission approaches to ethics (see http://cordis.europa.eu/fp7/ethics_en.html).

Thus, as for socio-contextual and ethical dimensions, we do not provide prescriptive ethical guidance, but we invite the designer of a system to take into full consideration a variety of socio-contextual and ethical dimensions while designing the system. Depending on the specificities of the system, we argue, the designer and the owner are the best persons to answer practical as well as ethical questions, and can justify his/her own choices according to some ethical insights.

In D2.2., we found out that the aims of the questionnaire as for the socio-contextual and ethical dimensions are as follows:

- To identify key legal stakes, ethical values and/or accountability issues at stake;
- To accompany development along the steps;
- To foster a reflection upon legal, socio-contextual and ethical, technical and accountability dimensions.

For the SALT user, the questionnaire approach has three core advantages. The first one is that it can take the SALT user through the process of conceiving, designing and implementing a SALT system, i.e. a system of surveillance. At each stage of development (see 2.2.), the user has questions to answer so as to better apprehend and grasp the legal, socio-contextual and ethical, technical and accountability dimensions of the system he/she is designing.

A second advantage is that the questionnaire crafted in SALT frameworks is thought of as a dynamic tool, which can be used at several stages of the process and to which is possible to come back and forth. While the questions appear to be sequential, it will be possible to "browse" through questions, make sure that the variety of dimensions is fully taken into consideration.

A third advantage is that SALT framework tools are flexible and can evolve over time, they benefit from the input of SALT experts, being understood that each user might potentially become an expert. Also, the knowledge-based used to make sound decision-making and full-fledged integration of legal, socio-contextual and ethical, technical and accountability dimensions can be broadened and enriched by the participants to the SALT systems, so that the tool itself evolves and gets refined over time.

2.2 A companion to the 3 stage-process

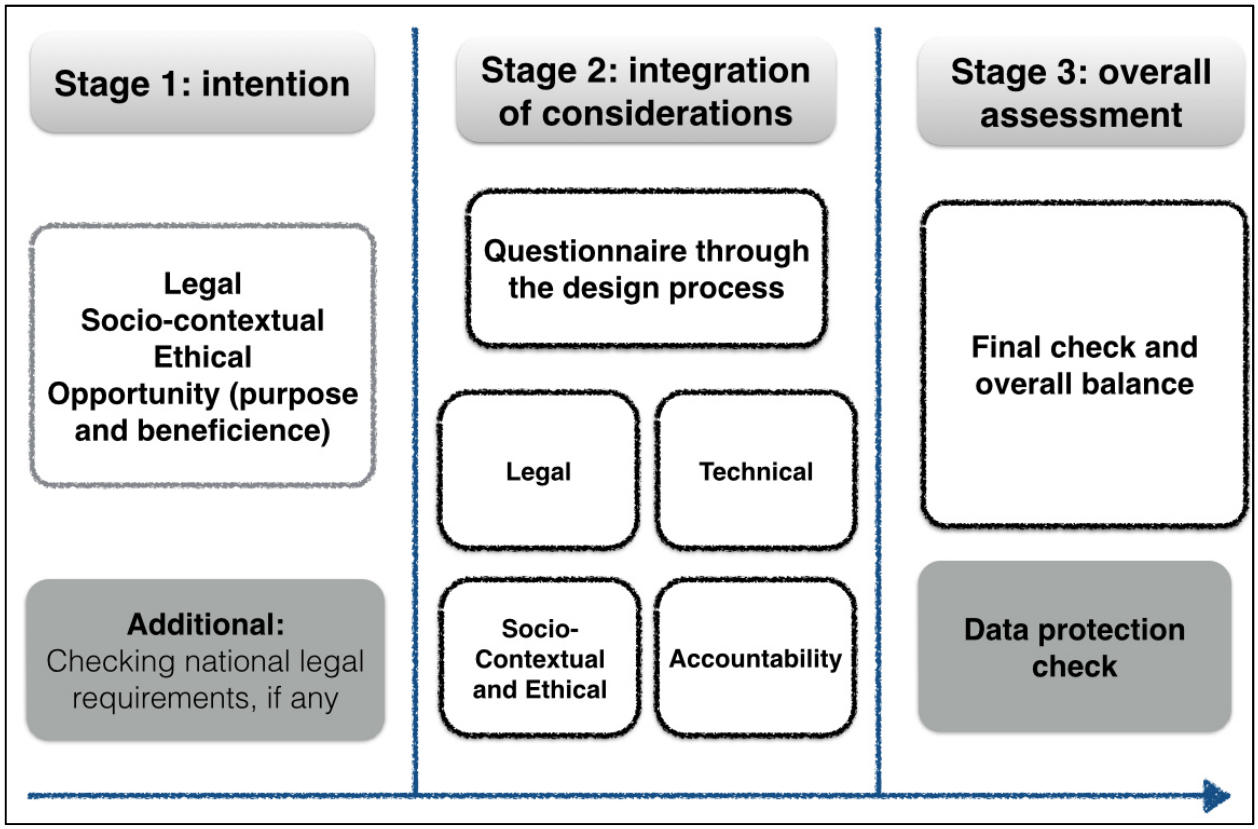


Figure 2 Three stage process for SALT Framework

Regarding socio-contextual, ethical and legal issues, we identify a three-stage process for the SALT framework. The caption above describes those three processes as the project of establishing a surveillance system evolves over time, from left to right. With respect to the SALT procedure, specific questions must be asked at different stages of the conception, design or implementation of the system. The purpose of those questions is to strengthen the legal, socio-contextual and ethical, as well as technical and accountability dimensions of the system. These ought to be taken into full consideration so as the system reinforces its good integration of those dimensions.

The first stage regards the intention of the purpose of a surveillance system. It should ask the question of the opportunity of installing the system that is making a general balance of its purposes in terms of proportionality and beneficence.

The second stage addresses different aspects throughout the design process, i.e. legal, socio-contextual and ethical, technical, and as for the accountability. All the questions are knowledge-based and represented as SALT instances in the SALT framework.

Finally, all the system is designed and answers to the questions have been provided, the third stage includes a final assessment of the overall system, with respect to its initial aims, and with final checks of legal requirements.

This three stage process is addressed mostly at the system designer and at the system owner. But, in order to be fully deployed, it needs to be as integrative as possible of other stakeholders, at each stage. The perspective on privacy issues, socio-contextual and ethical will be different for each relevant stakeholders.

While this three stage process might look very sequential, i.e. a little linear in scope, it is important to underline that this is not what the SALT framework achieves. All the contrary, the SALT framework is flexible and the SALT user can browse through the repository back and forth. There will be bridges and possibilities to move forward in the questioning as well as to come back to it.

To this extent, what we see is that SALT framework allow for a process of feedback loop and retroactions, so as to always fine-tune the legal, socio-contextual and ethical, technical and accountability relevance. In other words, the user will enter a learning mechanism through which he/she will become available to understand all these dimensions and take full considerations of what they entail for the system he/she is conceiving and designing.

3 Guidelines for creators of references

The knowledge in the SALT Repository is stored in the form of SALT references, as explained in D6.2 (in relation to biometric systems) and D5.2 (in relation to videosurveillance systems). Each of these references contains information regarding one or several privacy and/or accountability concerns. It is important to remark that since experts create SALT references, their content fully depends on them. It is the purpose of this section to address the guidelines to be followed by experts when creating a new reference.

3.1 One single reference template

This is the template used for the creation of references in the SALT Repository. This template has been prepared in closed collaboration between all different partners in order to take into account different knowledge. The template presented hereunder is aligned with the work in other work packages of this project (WP6 to WP5):

Field	Type	Description
Reference name	Mandatory	Name that serves to identify the reference, that should be as descriptive as possible. In case the references correspond to a law, an article, a report or any other official document, the name should be the title of that document. In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: *Organic Law 15/1999 on the Protection of Personal Data - Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*
Original language	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
Abstract	Optional	Brief summary of the contents of the reference *(~ 100 words maximum)* In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields).
Link to source	Optional	Link to the source of information in the original language
Link to translation	Optional	Link to the source of information translated to English
Official translation	Optional	[Yes, No] This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies).
System type	Mandatory	The system type to which the reference applies. *Possible values: Video surveillance systems / Biometric systems / All systems*
Geographical Scope	Mandatory	A first layer of context information, which will define the territorial scope of application. The SALT Framework Tool for the creation of references will provide a drop down list containing a set of predefined countries (by now, all the European countries and also the option "European Union" to cover all them). There is also the option "Any" for the cases where this information is not relevant for the reference (e.g. technical information).
Context	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference (*e.g. specific cases/conditions*

		where the reference is applicable).
Version	Mandatory	Version of the reference in the format vA.B. By default this field has the value: v0.1
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the reference
Creator	Automatic	Person responsible for the creation of the reference in the SALT Repository *(automatically filled by the SF Tool)*
Last update	Automatic	Date and time of the last reference update *(automatically filled by the SF Tool)*
***List of concerns** (privacy and accountability related concerns for surveillance systems)*		
Concern ID	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
Name	Mandatory	Title for the concern, which should give a brief idea of the contents or aspects covered by the concern. The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A text would probably include more than one concern. In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: Duty to inform - Deber de informar
Additional information	Optional	Extra information that helps readers find the concern in the source text.
Description	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc.
Category	Mandatory	Category of the concern, that can be one or several among this options: *Legal, Socio-Ethical, Technical.*
SALT Topics	Optional	SALT legal topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks. The list of defined SALT legal topics, and its mapping with the privacy principles indicated in ISO Standard 29100, is available in Table 2
Stage	Optional	Stage or stages of the SALT Process in which this concern applies. These are the stages defined and their goals: • **concept** (intention): selection of the most suitable solution to solve the stakeholder's problem; • **design**: elaboration of the system design according to the different requirements; • **development**: implementation of the system based on the defined specification; • **deployment**: set up the system in the stakeholder's environment; • **operation & maintenance**: use the system and ensure its correct functioning to satisfy stakeholder's needs; • **retirement**: shut down the system in a controlled manner.
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern.
Guidelines	Optional	Any guidance on how to include the concern in the stage of the system lifecycle in which the concern applies. This could be a concrete artifact or solution, a strategy or procedure, or just any tip about how to take this

		concern into consideration.
OCL Rules	Optional	One or several OCL rules that allow to verify that the system addresses the concern. The OCL expert needs to fully understand the meaning of the privacy/accountability concern for which the OCL rules are created. These rules will be used for the automated (or human assisted) validation of the concern it relates to, once its corresponding solution provided by the SALT reference has been implemented in the system design. OCL rules are only available for the design stage (in parallel with the UML profile).

Table 1: Template for the SALT References

SALT legal topic	ISO principle
Definitions	Terms and definitions, Actors and roles, recognizing PII
Fairness	n/a
Legal basis	Consent and choice; purpose legitimacy and specification
Purpose specification	Purpose legitimacy and specification
Data minimization	Collection limitation
Data Quality	Accuracy and quality
Data retention	Use, retention and disclosure limitation
Proportionality	n/a
Further use limitation	Data minimization; use, retention and disclosure limitation
Authorised disclosure	Data minimization
Sensitive data	
Data Subjects' rights	Individual participation and access
Data security	Information security ; privacy compliance
Accountability	Accountability
Transparency	Consent and choice; purpose legitimacy and specification; openness, transparency and notice
Data protection risks	Privacy compliance

Table 2: Mapping of ISO principles and SALT legal topics

3.2 A template compatible with different knowledge domains

If the references rely on a common template, each expert responsible for the creation of a SALT reference in its own expertise domain will follow the specific guidelines described in the following sub-sections.

3.2.1 **Guidelines for the creation of legal references**

Field	Type	Description
Reference name	Mandatory	The reference name shall be the full title of the legal document, whether it is a law, an opinion of a Data Protection Authority or caselaw. In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen.

		Example in the case of a legislation: *Organic Law 15/1999 on the Protection of Personal Data - Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal* ***Example of reference name of a caselaw:*** *Court of Justice, 8 April 2014, Digital Rights Ireland* ***Example of reference name of softlaw documentation:*** *Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies*
nd	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
Abstract	Optional	Brief summary of the contents of the reference *(~ 100 words maximum)* In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields). ***Example in relation to Directive 95/46:*** *The Directive provides for a set of rules that protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data. Its provisions have been transposed in all European Member States in national legislation*.
Link to source	Optional	Link to the source of information in the original language
Link to translation	Optional	Link to the source of information translated to English
Official translation	Optional	[Yes, No] This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies). It is especially important for legal references.
System type	Mandatory	The system type to which the reference applies. When this is a general legislation, the entry “all systems” may be relevant. When this is a specific legislation, it should be speciaified. *Possible values: Video surveillance systems / Biometric systems / All systems*
Geographical Scope	Mandatory	A first layer of context information, which will define the territorial scope of application. The SALT Framework Tool for the creation of references will provide a drop down list containing a set of predefined countries (by now, all the European countries and also the option "European Union" to cover all them). It is important to indicate for which jurisdiction the legal reference is relevant.
Context	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference (*e.g. specific cases/conditions where the reference is applicable).* This is relevant for legal references which shall include here a description of the material scope of application of the legislation. In case of caselaw, it may be relevant to recall the activities impacted by the decision.
Version	Mandatory	Version of the reference in the format vA.B. By default this field has the value: v0.1
Keywords	Optional	List of words or terms, separated by commas that serve to highlight the most relevant aspects of the reference.
Creator	Automatic	Person responsible for the creation of the reference in the SALT Repository *(automatically filled by the SF Tool)*
Last update	Automatic	Date and time of the last reference update *(automatically filled by the SF Tool)*

List of concerns (privacy and accountability related concerns for surveillance systems)		
Concern ID	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
Name	Mandatory	Title for the concern, which should give a brief idea of the contents or aspects covered by the concern. The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A single legal reference generally includes more than one concern. In the case of legislation, a concern will often coincide with a chapter/section of the law or an article when such law will prove to be very complex. In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: Duty to inform - Deber de informar
Additional information	Optional	Extra information that helps readers find the concern in the source text.
Description	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc.
Category	Mandatory	In this case it is automatically a *Legal reference*
SALT Topics	Optional	SALT legal topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks. The list of defined SALT legal topics, and its mapping with the privacy principles indicated in ISO Standard 29100, is available in Table 2**.** Here, the expert shall list the most relevant privacy principles to the concern.
Stage	Optional	Stage or stages of the SALT Process in which this concern applies. These are the stages defined and their goals: • **concept** (intention): selection of the most suitable solution to solve the stakeholder's problem; • **design**: elaboration of the system design according to the different requirements; • **development**: implementation of the system based on the defined specification; • **deployment**: set up the system in the stakeholder's environment; • **operation & maintenance**: use the system and ensure its correct functioning to satisfy stakeholder's needs; • **retirement**: shut down the system in a controlled manner.
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern. The expert shall provide a list of keywords relevant to the concern. This list may be identical or not to the SALt topics.
Guidelines	Optional	Any guidance on how to include the concern in the stage of the system lifecycle in which the concern applies. This could be a concrete artifact or solution, a strategy or procedure, or just any tip about how to take this concern into consideration.
OCL Rules	Optional	Not relevant for legal experts.

Table 3: Template for Legal References

3.2.2 **Guidelines for the creation of ethical references**

Field	Type	Description
Reference name	Mandatory	The reference name shall be the full title of the document, article or study. In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. ***Example in the case of an article:*** *Seven Types of privacy*
nd	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
Abstract	Optional	Brief summary of the contents of the reference *(~ 100 words maximum)* In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields). ***Example:*** *In their paper, Seven Types of privacy, those authors propose to extend the definition of privacy – using in a way this notion as a springboard or a lever – to any "specific elements of privacy which are important and must be protected", attempting "to capture the complexity of privacy issues within frameworks that highlight the legal, socio-psychological, economics or political concerns" that surveillance technologies present. They define their approach as **pro-active and protective** regards to privacy, "over-arching protection that should be instituted to prevent harms", offering "a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions infringements and problems."* *They identify their **taxonomy of types privacy** by contrast with **taxonomy of privacy harms** which they identify as being the result of a reactive posture regards to privacy, a "reactive highlighting of concerns or intrusions. It's worth noticing that the seven types of privacy retained in this taxonomy expand a former categorization of four types of privacy identified in 1997 by Roger Clarke. The main argument formulated by Finn, Wright and Friedewald in favour of the partial reworking and the expansion of this previous categorization is that the coming of new and emerging technologies and applications has meant to have new impacts of privacy in such a way "that previously unconsidered types of privacy now need to be addressed in order to adequately protect individuals' rights, freedoms and access to goods and services".* *Finn, Wright and Friedewald, while reworking Clarke's first classification, defined those seven types of privacy:* ***1.*** *Privacy of the person* ***2.*** *Privacy of personal behaviour and action* ***3.*** *Privacy of personal communication* ***4.*** *Privacy of personal data and image* ***5.*** *Privacy of thoughts and feelings* ***6.*** *Privacy of location and space* ***7.*** *Privacy of association*
Link to source	Optional	Link to the source of information in the original language

Link to translation	Optional	Link to the source of information translated to English if any
Official translation	Optional	[Yes, No] This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies). It is especially important for legal references and will not be relevant in most cases for ethical references.
System type	Mandatory	The system type to which the reference applies. ***Possible values**:* *Video surveillance systems / Biometric systems / All systems* ***In our example (Seven Types of privacy):*** *All systems*
Geographical Scope	Mandatory	A first layer of context information, which will define the territorial scope of application. The SALT Framework Tool for the creation of references will provide a drop down list containing a set of predefined countries (by now, all the European countries and also the option "European Union" to cover all them). ***In our example (Seven Types of privacy):*** *European Union*
Context	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference (*e.g. specific cases/conditions where the reference is applicable).* ***In our example (Seven Types of privacy):*** *Any*
Version	Mandatory	Version of the reference in the format vA.B. By default this field has the value: v0.1
Keywords	Optional	List of words or terms, separated by commas that serve to highlight the most relevant aspects of the reference. ***In our example (Seven Types of privacy):*** *Surveillance, privacy, Privacy impacts, Privacy harms*
Creator	Automatic	Person responsible for the creation of the reference in the SALT Repository *(automatically filled by the SF Tool)*
Last update	Automatic	Date and time of the last reference update *(automatically filled by the SF Tool)*
***List of concerns** (privacy and accountability related concerns for surveillance systems)*		
Concern ID	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
Name	Mandatory	Title for the concern, which should give a brief idea of the contents or aspects covered by the concern. The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A single reference can include more than one concern. In the case of sociological or ethical literature or sources, a concern may coincide with a chapter/section of an article when such art will prove to be very complex. In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. ***In our example (Seven Types of privacy):*** *Privacy of the person*
Additional information	Optional	Extra information that helps readers find the concern in the source text. ***Example:***

		Page number 4
Description	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc. ***In our example (Seven Types of privacy):*** *Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. According to Mordini, the human body has a strong symbolic dimension as the result of the integration of the physical body and the mind and is "unavoidably invested with cultural values". Privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society.*
Category	Mandatory	***In our example (Seven Types of privacy):*** *Socio-ethical*
SALT Topics	Optional	SALT topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks. The list of defined SALT topics, and its mapping with the privacy principles indicated in ISO Standard 29100, is available in Table 2**.** Here, the expert shall list the most relevant privacy principles to the concern. ***In our example (Seven Types of privacy):*** *Data protection risks*
Stage	Optional	Stage or stages of the SALT Process in which this concern applies. These are the stages defined and their goals: • **concept** (intention): selection of the most suitable solution to solve the stakeholder's problem; • **design**: elaboration of the system design according to the different requirements; • **development**: implementation of the system based on the defined specification; • **deployment**: set up the system in the stakeholder's environment; • **operation & maintenance**: use the system and ensure its correct functioning to satisfy stakeholder's needs; • **retirement**: shut down the system in a controlled manner. ***In our example (Seven Types of privacy):*** Concept; Design
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern. The expert shall provide a list of keywords relevant to the concern. This list may be identical or not to the SALt topics. ***In our example (Seven Types of privacy):*** Privacy of the person, definition
Guidelines	Optional	Any guidance on how to include the concern in the stage of the system lifecycle in which the concern applies.
OCL Rules	Optional	Not relevant for ethical experts.

Table 4: Template for the socio-contextual and/or ethical References

3.2.3 Guidelines for the creation of technical references

Field	Type	Description
Reference name	Mandatory	The reference name shall be the full title of the document, article, report or study. In case it is an evaluation or recommendation of an expert about a certain technical solution in terms of privacy, not based in a specific document, this field should indicate the technical solution described in the reference and a notion about the context. In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. ***Example in the case of an article:*** *Privacy by Design Solutions for Biometric One-to-Many Identification Systems* ***Example in the case of an expert evaluation:*** *Use of bodyprints for business intelligence in retail applications*
Original language	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
Abstract	Optional	Brief summary of the contents of the reference *(~ 100 words maximum).* It is important that the abstract hightlights the most important aspects contained in the reference. In the case of an evaluation or recommendation of a technical solution not supported by a specific document, the abstract shall contain as many details as possible about the topic addressed in the reference. In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields). ***In the example** (Privacy by Design Solutions...):* *Biometric one-to-many systems have been used for a variety of purposes, such as multiple enrolment prevention, watch list, access control, forensics, stranger identification, etc. While these systems often serve legitimate purposes, such as combating fraud or catching a villain, the rise of the ubiquitous use of biometrics can be viewed as an integral part of the emerging surveillance society.* *Biometrics, especially one-to-many systems, can pose some serious threats to privacy due to uniqueness, permanent nature and irrevocability of biometric data. However, it does not have to be that way. The same technology that serves to threaten or erode our privacy may also be enlisted to strengthen its protection. In particular, Biometric Encryption (BE) technologies, or, in more general terms, "Untraceable Biometrics" was proposed as a privacy-protective alternative to conventional one-to-one biometrics.* *In this paper, we apply a Privacy by Design approach to exploring new ideas and solutions that can lead to deployment of privacy-protective and secure biometric one-to-many systems. We show that new advances in BE can be complemented with other innovative solutions, such as Cryptographically Secure Biometric Architectures and Biometric Setbase/Weak Links. We present a case study of the first BE application using facial recognition in a watch list scenario at the Ontario Lottery and Gaming Corporation (OLG). We propose a cryptographically secure architecture for a one-to-many system using Blum-Goldwasser cryptosystem.* *These solutions can be combined with each other in the application specific*

		context in order to create a one-to-many system that addresses privacy, security and functionality issues, all the hallmarks of a Privacy by Design approach.
Link to source	Optional	Link to the source of information in the original language
Link to translation	Optional	Link to the source of information translated to English
Official translation	Optional	[Yes, No] This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies).
System type	Mandatory	The system type to which the reference applies. *Possible values: Video surveillance systems / Biometric systems / All systems* ***In the example** (Privacy by Design Solutions...):* *Biometric systems*
Geographical Scope	Mandatory	A first layer of context information, which will define the territorial scope of application. In the case of technical information, this field does not have much sense unless it refers to the use of a certain technology in a certain scenario related to a specific geographical context. In case the territorial scope is not relevant, just put "Any" in this field.***In the example** (Privacy by Design Solutions...):* Any
Context	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference. In a technical context, it is important to indicate in this field the specific conditions or scenarios in which the reference can be applied, and any explanation required to understand in which cases this reference could be considered. ***In the example** (Privacy by Design Solutions...):* *The solutions proposed in this document can be applied to any biometric system performing one-to-many identification.* *Identification refers to the ability of a system to uniquely distinguish an individual from a larger set of centrally stored biometric data or what is often referred to as a one-to-many match. Identification systems require storing large amounts of data and, in general, are more prone to errors.*
Version	Mandatory	Version of the reference in the format vA.B. By default this field has the value: v0.1 ***In the example** (Privacy by Design Solutions...):* V0.1
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the reference. As this field is used to find references in the repository, it is important to include in the list the main topics contained in the reference, and also think in which terms could a person use to look for this specific reference. ***In the example** (Privacy by Design Solutions...):* *Biometric systems, identification, privacy by design, recommendations, technical solutions*
Creator	Automatic	Person responsible for the creation of the reference in the SALT Repository *(automatically filled by the SF Tool)* ***In the example** (Privacy by Design Solutions...):* Visual Tools
Last update	Automatic	Date and time of the last reference update *(automatically filled by the SF Tool)* ***In the example** (Privacy by Design Solutions...):*

		10/4/2015
List of concerns *(privacy and accountability related concerns for surveillance systems)*		
Concern ID	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool) ***In the example*** *(Privacy by Design Solutions...):* *PBD.BIOID.2*
Name	Mandatory	Title for the concern, which should give a brief idea of the contents or aspects covered by the concern. The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A text would probably include more than one concern. In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. ***In the example*** *(Privacy by Design Solutions...):* *Database separation*
Additional information	Optional	Extra information that helps readers find the concern in the source text. ***In the example*** *(Privacy by Design Solutions...):* Page 2
Description	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc. As technical references are mainly addressed to users with technical background, it is important to clarify as much as possible the non-technical aspects related to the concern, for example, the privacy issues, providing links to external sources of information or to a certain taxonomy or reference stored in the SALT Repository if necessary. ***In the example*** *(Privacy by Design Solutions...):* *To protect the privacy in biometric 1:many systems, a database separation was proposed in one of the versions of the Biometric Documents Identification Law of 2009 in Israel and also in the new ISO/IEC standard. In these scenarios, the anonymous database of biometric templates is stored separately from the database containing personal information (PI) of the users. Both databases are administered by separate government entities. The databases are linked only by digital identifiers. Upon a positive biometric identification, a digital identifier is released and corresponding PI is retrieved from the second database.* *While the idea of database separation is a step in right direction, this is not enough. It is obvious that, in fact, only legal measures provide protection of privacy. Both biometric and personal information are still fully under the government control.* *Moreover, the anonymous biometric database can be linked with other biometric databases because of the permanent nature of biometrics.*
Category	Mandatory	Category of the concern, that can be one or several among this options: *Legal, Socio-Ethical, Technical.* ***In the example*** *(Privacy by Design Solutions...):* *Technical*
SALT Topics	Optional	SALT legal topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks. The list of defined SALT legal topics, and its mapping with the privacy principles indicated in ISO Standard 29100, is available in Table 2

		Normally, the technical references address data protection risks associated to a certain technology, or one of the topics associated to the processing of data: • Data minimization (e.g. machanisms to control the collection of data) • Data quality (e.g. mechanisms to ensure data quality) • Data retention (e.g. mechanisms to ensure that the data is not kept for more time than necessary) • Further use limitation (e.g. mechanisms for access control) • Data subject's rights (e.g. mechanisms to let users access their data securely without compromising the privacy of other users) • Data security (e.g. mechanisms for data protection) ***In the example** (Privacy by Design Solutions...):* *Data security, Data protection risks*
Stage	Optional	Stage or stages of the SALT Process in which this concern applies, or in which it should be considered. This field should be easier to fill by technical experts, as they are more familiar with system lifecycles. These are the stages defined and their goals: • **concept** (intention): selection of the most suitable solution to solve the stakeholder's problem; • **design**: elaboration of the system design according to the different requirements; • **development**: implementation of the system based on the defined specification; • **deployment**: set up the system in the stakeholder's environment; • **operation & maintenance**: use the system and ensure its correct functioning to satisfy stakeholder's needs; • **retirement**: shut down the system in a controlled manner. ***In the example** (Privacy by Design Solutions...):* *Design*
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern. Again, as this field is used for searching purposes, the technical expert should indicate here the main topics addressed in the concern and which search terms should lead to this reference. ***In the example** (Privacy by Design Solutions...):* *Biometric data, biometric templates, biometric systems, storage, technical measures*
Guidelines	Optional	Any guidance on how to include the concern in the stage of the system lifecycle in which the concern applies. This could be a concrete artifact or solution, a strategy or procedure, or just any tip about how to take this concern into consideration. ***In the example** (Privacy by Design Solutions...), there is no specific guideline for this concern, as it is just a reasoned concept that designers can consider or not for the design of a one-to-many identification system.*
OCL Rules	Optional	One or several OCL rules that allow to verify that the system addresses the concern. The OCL expert needs to fully understand the meaning of the privacy/accountability concern for which the OCL rules are created. These rules will be used for the automated (or human assisted) validation of the concern it relates to, once its corresponding solution provided by the SALT reference has been implemented in the system design. OCL rules are only available for the design stage (in parallel with the UML profile).

		In the example *(Privacy by Design Solutions...), again, as there is no concrete artifact to be implemented, it is not possible to define an OCL Rule. We could just create an attribute to indicate the contents of a data storage and check if the templates are separated from the personal information, but it is not mandatory, it is just a recommendation for designers.*

Table 5: Template for the technical References

4 Guidelines for users by domain

In this section, we introduce the actual guidelines domain by domain. First, for socio-contextual and ethical dimensions; second, for legal dimensions; third, for technical dimensions. Then, in the fourth subsection, we address the dimensions of accountability, which is more encompassing than the others.

4.1 For Socio-contextual and ethical dimensions

4.1.1 User roles

It is very difficult to identify one particular "user" for socio-contextual and ethical dimensions because, by definition, those dimensions pervade the whole process of conceiving of, designing and implementing a surveillance system in public spaces.

To this extent, either the designers of SALT systems, the public at large or concerned associations can address those dimensions at some point or the other of the process. In short, taking into account the socio-contextual and ethical dimensions potentially concerns any stakeholder.

However, for the purpose of writing the guidelines of this deliverable, we must distinguish between direct target users and indirect target users. Direct target users are surveillance system designers, surveillance system owners and surveillance system operators (for a definition and more information about those categories of users, see D2.2, 1.2.2, pp. 16-17). For those two categories are the forefront of providing decisive input into the design and implementation of surveillance systems through which the socio-contextual and ethical dimensions can best be taken into account.

The questionnaire is primarily crafted for those who are developing or intend to develop an information technology project, policy or program that have socio-contextual and ethical implications, assuming that « surveillance » and « security » related projects always do have such implications.

Indirect target users, as for them, may and should be included as broadly as possible at all stages of development of the system. Those include, but are not limited to, surveillance system maintenance operators, surveillance system user, and surveillance system contractor. But somehow it must reach out to a broader public than only the one "using" the system. It could rather include concerned individuals and also the one which are impacted by the system without necessarily using it. Lastly, indirect target users for socio-contextual and ethical dimensions of SALT framework also include data protection authorities and civil society organizations.

In this regard, the questionnaire may also be of interest for policy-makers or projects managers and, more broadly perhaps, « should target stakeholders interested in or affected by the outcome » (Wright, p. 201). However, in this case, the interest of the SALT framework is more indirect and its inputs can be used to inform the cases which are discussed.

4.1.2 Purpose and limits

Before we get to the guidelines for socio-contextual and ethical dimensions, it is important to remind a few methodological constraints and limits. For the user, applying the SALT framework is not mandatory. In this way, one must keep in mind that the user may not want to use it, which is the reason why the framework is an invitation rather than an obligation. To this extent,

the framework has to be made as clear as possible, user-friendly and provide useful added value and incentives to use. This is the purpose of these guidelines.

It has already been stated in D2.2. that applying SALT frameworks to the design and implementation of surveillance systems in public space shall to no extent lead to some automated forms of decision-making or binding compliance. Instead it shall enrich the process of designing such systems. It is important for the SALT system designer to bear this in mind so as not to expect out of the SALT framework something that the system cannot provide.

For this reason, the expertise in socio-contextual and ethical dimensions is more of a toolbox, a companion to the process of developing a SALT system. It ought to accompany the user along such processes. In this respect, the user must understand that the socio-contextual and ethical dimensions must come from him/herself, not from the socio-contextual and ethical expert. In other words, the expert needs not to say what such dimensions "are" but instead suggest a few key points of the socio-contextual and ethical dimensions. These dimensions, the SALT user should keep them in mind along the process and offer to it his/her own answers.

In particular, it can be a systematic manner of understanding and dealing with the Charter of Fundamental rights. The operationalization of the principle of proportionality in the questionnaire has been one of the core tasks dealing with this issue (see *infra* section 4.2). Usually, the socio-contextual and ethical dimensions rely on existing references so as not to reinvent solutions that already exist and are widely in use, such as David Wright's ethical impact assessment. An extended version of the socio-contextual and ethical questionnaire has been drafted in D2.3., which encompasses the questions and dimensions the user may want to be sensitised to and provide his/her own answer for.

The SALT user now understands that reflecting upon those dimensions will by any means enrich the whole design process and it will make it socio-contextually and ethically more sound, more relevant. But it will not carry out an automated form of social acceptability, neither can polls or public opinion surveys do. Because the social acceptability of surveillance systems always depends on local settings, of particular situations and that there are no rules that allow saying that one kind of system is acceptable or unacceptable in all situations. This is also very important for the SALT user to figure out.

Lastly, as the good functioning of SALT frameworks rely upon its users and their contributions, it is very important to recall that the responsibility of the good use of the SALT frameworks depends on its uses. For this reason, it is very important that the use takes it seriously and apply it in all consciousness and with due care for those complex dimensions. The following guidelines are designed to underscore this importance and offer a set of methodological hints, which can ensure that the socio-contextual and ethical dimensions (as seen in D2.2.) will be most adequately taken into account.

4.1.3 **Methodological guidelines**

4.1.3.1 Inclusiveness of the process

First of all, the questionnaire-based approach is not incompatible with the other tools mentioned in D2.2. (section 3.1.1.1.). While coping with socio-contextual and ethical issues, one would rather enlarge as much as possible the scope of ethical reflection. Usually, the more encompassing, inclusive and participative the approach is, the best is the outcome of the socio-contextual and ethical process.

This happens because a broad variety of perspectives can be put together and each of them brings its own values and viewpoints on those matters. In such a way, the diversity of perspectives feed into one with the other, instead of being in competition to determine “the” only right ethical solution. Instead, as we already stated, ethics and socio-contextual dimensions are a process. However, we also acknowledge that this process needs to be cost efficient, especially at early stages of development where it targets the actual designer of the system.

That being said, the SALT framework, in particular the SALT questionnaire, has integrated some participatory tools in view of involving stakeholders and enhance the views on socio-contextual and ethical dimensions.

4.1.3.2 Dynamic use

The questionnaire requires a dynamic use throughout the system design process, from the initial intention to actual implementation, and all the socio-technical decisions that are made in between. This fits with the three-stage process described in section 2.2. For the user, the implication is that socio-contextual and ethical dimensions should be reflected upon, and integrated, throughout the whole process of conceiving, developing and implementing a surveillance system.

In social sciences is commonly used the metaphor of the stream; a system is “downstream” at very early stages of development, when someone who has the capacity to do so decided the system should get designed and implemented ; “midstream” refers to all the experimental processes and steps taking place during the development phase; SALT framework operates mostly between those two first stages of development, even though it plans a short review process at the end of the development stage; lastly, “upstream” denotes a system which is ready for installation, and when it is most relevant to engage widely with society “at large”, and stakeholders.

In this respect, the SALT questionnaire shall be a guide that takes the user throughout the different stages of developing a SALT system. It accompanies the development of a particular system throughout its « technological trajectory », from early premises to end-of-pipe system. In this respect, it needs constant reviewing all along the way.

4.1.3.3 A closing procedure

The process should be as inclusive as possible, since socio-contextual and ethical dimensions require broad participation. However, participation necessarily results in conflicting views upon what ethics are or should be, what they entail or what guiding principles they should follow. In other words, it does not work univocally or in a unidirectional way. Instead, it involves to open up spaces of discussion where all those concerned, affected and targeted by a certain decisions will be consulted. It is a very demanding process.

And yet, while the process must be as encompassing as possible, some decisions have to be made. A certain degree of consensus must be reached in order for the system to work at some point. In D2.2. we referred to the need of establishing a “shared language” among the different system users and stakeholders involved in the process of discussing the socio-contextual and ethical dimensions. This does not mean that the consensus to be found is total, but instead that

some level of consensus needs to be reached. In other words, depending on the situations, some room must be left to disagreement.

In this respect, while coping with the socio-contextual and ethical dimensions, it is very important to delineate a “closing procedure”. Such a procedure is a formal moment appointed in order to put together the different views and positions together and make clear choices entrenched in each of these views. One understands that those decisions cannot necessarily entail each and every of these positions, but needs to find a fair level of inclusiveness. It is very important that this moment is planned and formalized somehow, preferably at the closing of the different stages exposed above (see 2.3.) through the publication of a report. The SALT questionnaire has taken this aspect into account and the extraction and publication of a report is one of the core goal of the SALT framework.

4.1.3.4 Situating the system

Socio-contextual and ethical dimensions always depend of the specificities of the current system that is being designed. However, ethical guidelines and principles do have a generic dimension (unlike the case of law to a large extend), although some of the questions raised will be more relevant than others depending on the proposed system at stake (for instance privacy of the person will have a particular salience in the case of biometrics).

In this respect, it is very important not to use ethical considerations in a straightforward manner, because these principles and guiding norms have to find articulations with the places and situations where surveillance systems will be applied. For each case, the way these principles will be apprehended, understood and enacted will vary. From place to place (it can be a country, a village, a neighborhood, a mall or an airport), ethical considerations will have different extensions and depend on many parameters.

In this respect, the SALT framework and SALT questionnaire tries to include specific recommendations as to the involvement and consultation of stakeholders in different contexts. A questionnaire and recommendations regarding the consultation of minors or employees have been prepared (see Annex 3).

4.1.3.5 Principle of delegation

Sometimes, the socio-contextual and ethical dimensions are not easy to grasp for the lay user, i.e. the principle of autonomy of the person. It is not always clear what it entails precisely, what it refers to, and so on. For this reason, it is encouraged to refer or to out-source some expertise on these dimensions. SALT References frameworks offer some knowledge and insights, but there might be some questions or concerns left out of scope, which is why the SALT user may want to enrich the knowledge-base by calling for some external additional expertise. This knowledge produced to fit to the situation can then be used to feed the SALT references.

In this case, we use a very extended notion of “expert”. The “expert” may very well be the citizen, the client, or the person who will be somehow targeted or affected by the surveillance system, provided that this person has anhistory, an opinion and possibly political statements to make about the system which should be put into place. In that sense, referring to external expertise perfectly fits with the inclusiveness of the process.

But here, it takes a different form. Here, it means that the system designer and/or owner who uses the SALT framework may very well recognize specific points of the system upon which he desires to delegate the decision to be made to the relevant external experts.

4.2 For the legal dimension

4.2.1 Main goals of the SALT Questionnaire

4.2.1.1 Integrate both high privacy and data protection standards

The right to privacy and the right to data protection are distinct rights, which are nevertheless closely related. The protection of personal data must be considered with regard to its filiation with the right to privacy. In the SALT framework, the right to data protection is not an end *per se* but rather is an instrument to the service of the protection of private life of individuals. Our approach therefore consists in integrating both rights.

4.2.1.2 Turn the principle of proportionality from theory to practice

A major goal of the SALT questionnaire is to operationalize the proportionality principle in an on-going process and not as an initial or final one-shot assessment. In this way, the data protection requirements (purposes, minimisation et cetera) will all play a role in the operationalization of the general principle of proportionality in practice. Such operationalization has been done in particular through the preparation of a specific questionnaire drafted for biometric systems. The three stages process of the questionnaire aims at integrating the proportionality requirement at all different stages of the decision/design process of a biometric system.

4.2.1.3 What can SALT users expect from the SALT framework

The SALT framework is a tool destined to help interested stakeholders in developing biometric systems to follow a thorough approach taking into account privacy and data protection standards at different stages of the design process of the system.

However, the use of the SALT framework does not guarantee that a given surveillance system complies with the law and does not consist in a fully developed data protection compliance check. The validity of a given surveillance system should always be assessed by lawyers.

4.2.2 Step-by step methodology

4.2.2.1 Stage 1 — "Opportunity"

Goal: This first stage focuses on the objective to help deciders (in general the future surveillance system owner) in assessing, in a preliminary stage of the decision-making and design making of a surveillance project, the overall proportionality and legitimacy of a project in relation to the stated purposes. A series of questions relating to the "Purpose(s)", "Legitimacy" and "Proportionality" of the project is proposed. Under each question, the questionnaire includes explanations in order to help the deciders to understand what kind of answers they are expected to provide or the conditions they should satisfy.

Most importantly, this first part of the questionnaire brings *an evaluation dimension*: under this approach the questionnaire tries to evaluate the overall proportionality of a biometric system on the basis of a limited number of essential criteria. This is where the questionnaire intends to provide an automated impact evaluation of a biometric system. Such an approach is very innovative, since it remains widely unfamiliar to lawyers. It is the purpose of Annex 1 of this report to explain how those criteria have been identified and selected and to which extent they may provide a useful preliminary privacy impact assessment of a biometric system. We will explain why and how France's policy in this respect has been extensively analysed and used as a relevant case study for the identification of potential European criteria and which criteria have been retained for the purposes of our privacy impact evaluation (Annex 1).

Interested stakeholders: the organization at the initiative of the surveillance system (surveillance system owner) and his lawyers.

Format: questionnaire with associated explanations/recommendations.

Expected effects: At the end of the first phase, the tool shall automatically generate a preliminary assessment of the proportionnality of the system envisaged. The orgnaisation will be aware of the level of impact (*low, medium, high, very high*) that the intended system is likely to have on individual's rights. The organization at the initiative of the implementation of a surveillance system should start to have a primary view over the legitimacy and necessity to recourse or not to a biometric system for the stated purposes/objectives.

Where systems will be likely to have a *low* or *medium* impact on privacy and data protection, the organization will be given some recommendations to minimize the risks, if any. Where the system will be likely to involve a disproportionate interference into individual's rights, the SALT questionnaire will recommend the adoption of alternative systems. For instance, in case of insufficiently robust legitimate ground (e.g. Weak consent for example), the system will recommend to ensure the collection of a valid consent.

The overall proportionality test proposed also allows to question, in a first stage, the rationale conducting an organization to envisage a biometric system, instead of other means, to achieve the stated purpose(s). Obviously, such assessment is only preliminary. Assessing the proportionality of a system requires consideration of all functioning aspects of the system.

If the results of such assessment prove to be sufficiently robust (*low* or *medium* impact on privacy and data protection), deciders should turn to national legal requirements to see how the technology is (or not) regulated.

4.2.2.2 Intermediary stage: checking national legal requirements

Goal: The objective is to identify whether there are specific national requirements applicable to the intended surveillance system. If any, such requirements should be taken into account as a priority. In this phase, lawyers shall use the legal references of the SALT framework in order to identify the national requirements.

Interested stakeholders: lawyers

Format: Legal references regarding national requirements in relation to a specific technology, if any

Expected effects: Where the national law of a given Member States will be found to provide specific requirements, these should be taken into account as a priority. On the contrary, if

national law provides no specific requirements, the organisation should turn to the second stage of the SALT framework entitled “Design”.

4.2.2.3 Stage 2: “Design”

Goal: The purpose of the second stage of the questionnaire is to assist designers to take into account relevant European standards of data protection in absence of specific and prescriptive national requirements. The SALT questionnaire is here based on European standards and guidance; in particular Opinions of the European group gathering all Member States Data protection Authorities, the so-called Working Party 29.

Interested stakeholders: the surveillance system owner, the surveillance system designer, and lawyers.

Format: questionnaire with associated explanations/recommendations.

Expected effects: In this phase, systems owners and system designers fulfill the questionnaire, which allows them to check that essential aspects likely to have an impact on the proportionality of the system have been taken into account. The Working Party 29 has not provided strict guidance of interpretation with respect to each data protection principle in relation to each possible application in practice. This is why the questionnaire and accompanying information/recommendations can only contribute to “assist” deciders and designers to adopt a reflexive approach with respect to the intended surveillance system. The use of the questionnaire “design” does not ensure that a system complies with the law. However, it provides useful assistance to decision making regarding a system.

4.2.2.4 Stage 3: Final balancing

Goal: In a third stage, the SALT questionnaire aims at questioning the final balancing of the interests at stake. It is inserted in the final stage of the SALT in order for stakeholders to demonstrate their awareness regarding the impacts of the surveillance project on individual’s privacy and data protection rights. Such a question should be answered taking into account all aspects of the surveillance project.

Interested stakeholders: the surveillance system owner, lawyers

Format: questionnaire

Expected effects: Making the effort to consider, in a final stage, the achieved balance of all interests at stake in a given surveillance project constitutes very valuable information for potential external auditors of the systems. Moreover, thoughtful efforts to answer this question could then be used either in view of producing a privacy & data protection impact assessment, or as “accountability information”.

4.2.3 Out of scope of the SALT framework: data protection and other compliance check

To be complete, the “design” phase should be supplemented by an exhaustive data protection compliance check, which however falls outside the scope of the SALT framework. Such an exhaustive data protection compliance check should be supplemented with other legal

compliance check (other constitutional requirements, labour law, administrative law) according to the circumstances.

The SALT framework and its questionnaires do not include such exhaustive “data protection (and other legal) compliance check” although such legal analysis is absolutely necessary before the implementation of a surveillance system. Such legal compliance check is the task of the lawyer of the organization.

In blue: steps covered by the SALT questionnaire
In grey: steps not entering within the scope of the SALT questionnaire but for which recommendations are mentioned

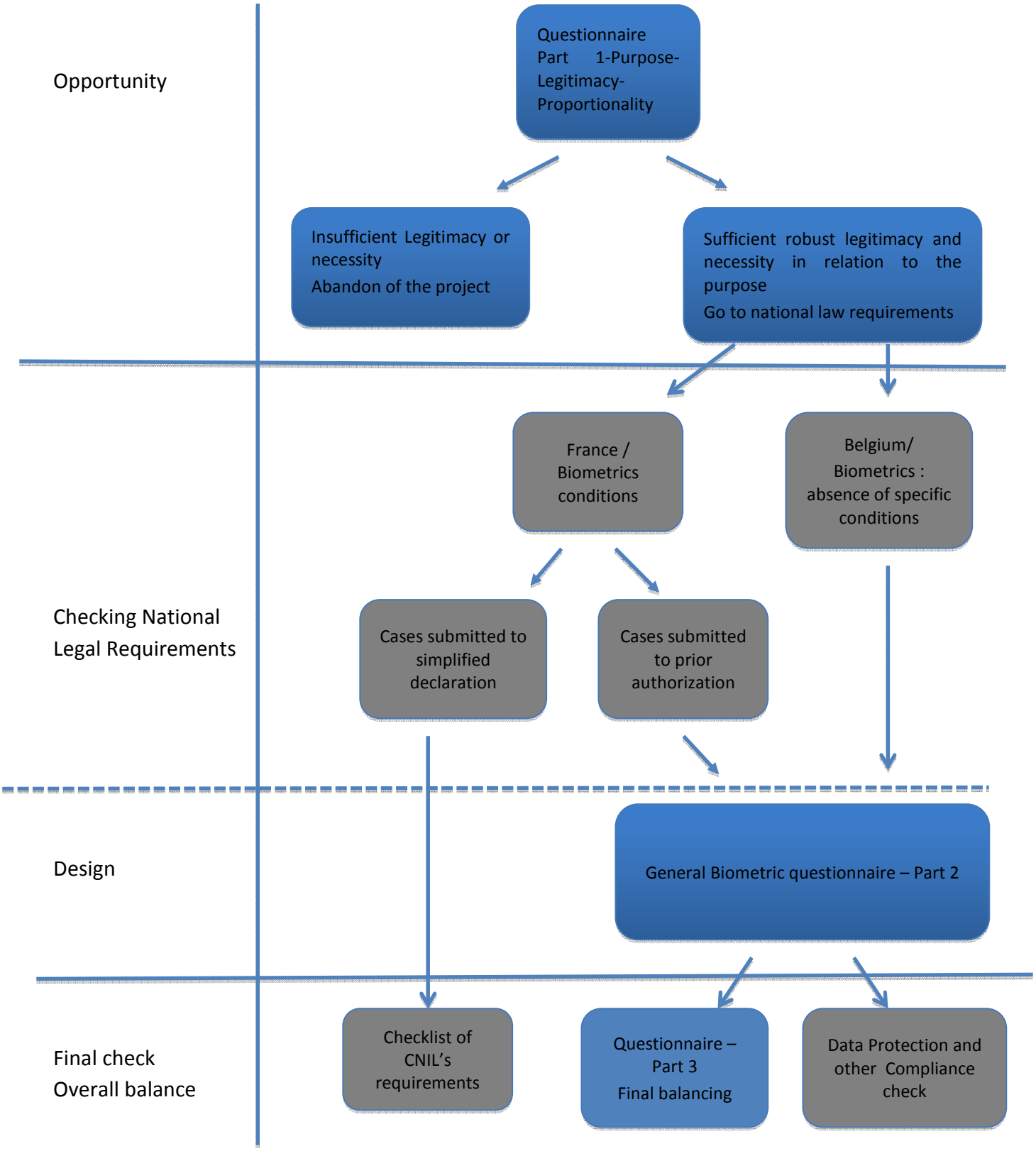


Figure 3 Overview of the use of the SALT framework from a legal perspective in relation to biometric systems with the examples of France and Belgium

4.2.4 The SALT framework in process: examples taken from the biometric questionnaire

In this section, we present three examples of uses of the SALT framework for the development of a biometric system. These three examples illustrate the process described in figure three above.

4.2.4.1 Use case n°1: installation of a biometric system to control access to school restaurant

The director of a school in France intends to put in place a biometric system to control access to the school restaurant.

Opportunity:

The director, with other interested stakeholders assesses the "opportunity" of the biometric system by answering to the first stage of the legal questionnaire. He is invited to argue on which legitimate ground the biometric system will rely, the purpose and necessity of such system. The director intends to use a fingerprint system with a centralized database. The impact evaluated is likely to be "*very high*".

Checking of national legal requirements:

After having reached a consensus within the Administration Council concerning the "opportunity" of a biometric system, the director consults the SALT framework and references to be aware of legal constraints applicable to such kind of systems in France. He finds out that the use of hand geometry to control access to school restaurants has been the object of a "Unique authorization" by the CNIL. They decide to opt for this specific biometric technology and to follow strictly the conditions established by the CNIL in AU-009 in order to implement quickly, rapidly and with legal certainty the biometric system.

4.2.4.2 Use case n°2: installation of a biometric system to control working time of employees

In France, an employer envisages to recourse to a biometric system in order to control the working time of his employees.

Opportunity:

Using the questionnaire, the employer's lawyers face difficulties in choosing the proper "legitimate ground" for such a biometric system (please see Q.2. and its explanations in annexe).

The questionnaire invites the organization to provide some explanation as to which "legitimate interests" are at stake in controlling the working time of employees. Indeed the questionnaire suggests three categories of "legitimate interest": i) legitimate of the organization only; ii) legitimate interests of the organization and of third; iii) legitimate public interest. The organization believes that the biometric system relates to both interest of the organization and of third. They intend to rely on a verification system with a local storage of fingerprint on an individual device held by the employees. The evaluation results mention a *low* impact on individual's rights. They decide to go on.

Checking of national legal requirements:

At the time of checking national legal requirements, the SALT framework contains specific information regarding the use of biometrics for time control & time management of employees. They find out that the CNIL, as a rule, does not consider such systems as proportionate. The CNIL has systematically refused the use of any kind of biometrics for purposes of controlling the working time of employees. In this context, the employer decides it is useless to notify an authorization request to the CNIL and decides to abandon the project. Instead, a traditional system of working time control (without biometrics) is prevailed.

4.2.4.3 Use case n°3: installation of a biometric system to control access to an amusement park

In France, the owner of an amusement park envisages to install a biometric system to control access to the premises of the park in order to prevent fraud. The Park counts about 4000 subscribers. Presently, subscribers access to the Park with a card and an identifying number. Anyone having such a card can access the Park although he is not a regular subscriber.

Opportunity:

While assessing the "opportunity" of the system, the owner of the Park does not invoke a security interest. Rather, the objective would be to limit the risks of fraud and protect the financial interests of the company. Following the SALT questionnaire/recommendations regarding "Legitimacy", the owner is directly invited to check whether data subject's consent requirement will be respected. Indeed, it is a formal requirement to install the biometric system control of access to the Park. Following the conditions explained in the SALT questionnaire, the owner decides to turn to a facultative enrollment, with the possibility, for subscribers, to withdraw at any time. The system owner envisages the use of a database with stored fingerprints of customers. Because of the evaluation results (very high impact), the owner of the amusement park modifies his initial approach and opts for a verification system with a decentralized storage of the biometric characteristics?.

Checking of national legal requirements:

After having checked national requirements, it appears that the intended biometric system is submitted to the prior authorization of the CNIL. A prior authorization request will be prepared. In order to improve the quality of the authorization request, the owner invites the system designer contractor to thoroughly follow the SALT questionnaire to design the system.

Design: Following the decision of the system owner to implement a biometric system on a facultative basis, the system designer then uses the SALT questionnaire to design the system with respect to all aspects of the system: type of biometric system, suitability and necessity; enrolment, matching, access/disclosure conditions, technical measures, storage, retention duration, erasure and security measures. For each aspect of the system, the questionnaire provides useful recommendations and help the designer to make the appropriate choices.

4.3 For Technical dimensions

The SALT Framework provides guidelines and tools for the development of both biometric and video surveillance systems, and there is no need to use a specific framework depending on the type of system as explained in D6.3. That said, it is important to point out that not all the contents stored in the SALT Repository can be applied for all type of surveillance systems. This is mainly because

biometric systems are considered more intrusive due to the nature of the data collected, and they are normally regulated by specific legislation or recommendations, requiring a more exhaustive assessment of the procedures and measures implemented for privacy and data protection. However, the use of the different tools and their application to the development of systems is similar for the different types of surveillance systems.

In order to understand how and when to use the different SALT resources, we should review first the process defined for the development of SALT compliant systems, which is depicted below. This design process strongly depends on the system development lifecycle used by the company producing the system, being independent from the type of system developed.

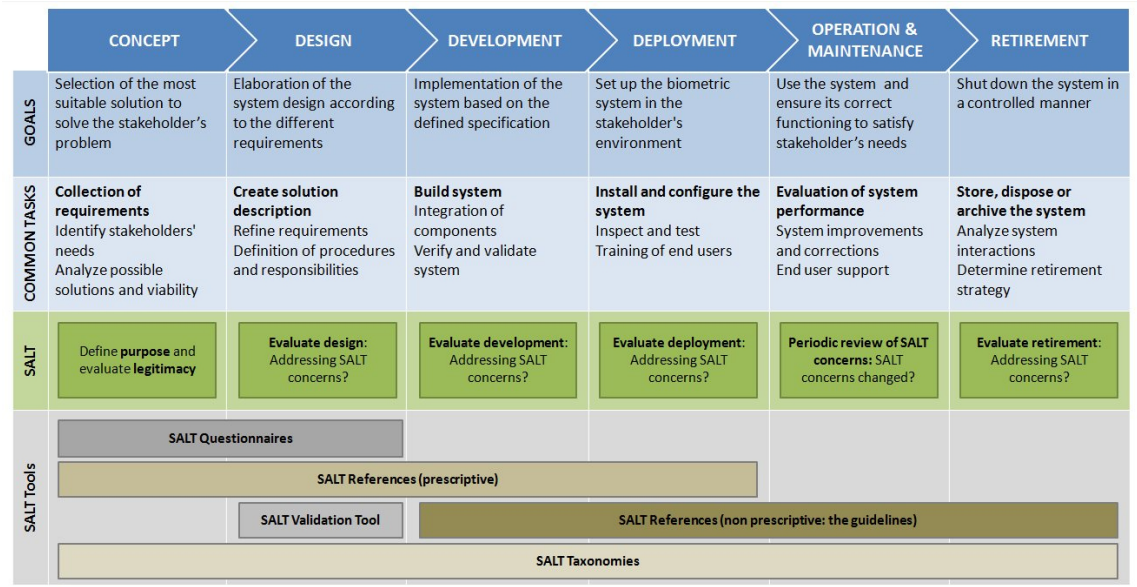


Figure 4: SALT compliant process for surveillance systems

This diagram shows the different stages of any system lifecycle including their goals, examples of tasks that are carried out in each stage, that also depend on the way of working of each company, the additional tasks that have to be performed to ensure that at the end of the process the system obtained addresses the main privacy and accountability concerns (SALT), and the SALT resources available in each case (SALT Tools). These stages are:

- **Concept stage**, in which the stakeholder's problems are analyzed in order to select the most suitable solution.

  In order to integrate privacy and accountability in this stage, it is essential to define clearly the purpose of the system and evaluate its proportionality and legitimacy. A person with certain legal expertise should perform this assessment, but it is also important to involve a technical expert in this stage to analyze the viability of the possible solutions from a technical point of view. It is not necessary to decide yet all the components and mechanisms that will be implemented, but it is important to have at least an idea about how the system can be configured and the type of data that will be collected and processed, as the collection and processing of data has to comply with the existing legislation.

  The SALT Framework provides questionnaires to guide the Privacy Impact Assessment and facilitate the evaluation of the need and proportionality of the system. Besides, the SALT Repository may include several references providing guidance for this stage of the

process, and also information of the data protection risks associated to different technologies.

- **Design**: once the system purpose has been evaluated, it is time to specify the strategy to follow to produce the system that will fulfill that purpose.
  The system design has to be evaluated in order to check if it addresses the main privacy and accountability concerns before the development phase, and in case the system design does not fulfill a requirement it should be reviewed and changed (if possible). In this evaluation at least a person with technical profile is required, but it would also be good to involve other type of experts from different fields (socio-ethics, legal, etc.) to ensure that the system design takes into account concerns of a different nature.
  Apart from the questionnaires and the SALT References, the SALT Framework provides another tool for the validation of system designs that highlights the main privacy and accountability concerns filled (and not filled) by a given design.

- **Development**: implementation of the system based on the design specification elaborated in the previous phase.
  This stage is basically technical, and thus carried out by a technical team (e.g. system designers/developers). The most important issue in terms of privacy and accountability is to check at the end of the stage that the different system components behave as expected, particularly the operations related to the collection and processing of data.

  The SALT Framework can also provide guidance for this stage in the form of SALT References.

- **Deployment**: the goal of this stage is to set up the biometric system in the stakeholder's environment. This work includes the installation of the system in the target location, its configuration and other supporting actions such as user training. At the end of this phase, the system is fully operational according to the defined requirements.
  The references stored in the SALT Repository can also provide some guidelines for this stage, such as legal requirements that have to be fulfilled before using the system for surveillance (e.g. how to install and position the cameras).

  In this stage, at least the stakeholder (DC), the installer and the surveillance service provider (SSP) are involved. It is not only important to set up correctly the system in the deployment stage, but also to prepare the documentation required (e.g. system manuals, privacy policies...), and define the responsibilities and procedures related to the processing of the data stored in the system.

- **Operation & maintenance**: in this stage the system operates for the purpose it was built, and it is monitored in terms of performance and availability to ensure that it works as expected and that it does not become obsolete.
  The operators of the system and the system administrators are normally in charge of these tasks.

  There can also be SALT references in the SALT repository providing guidelines for this stage, for example, recommending certain procedures or technical mechanisms to facilitate the maintenance of the system taking into account privacy and accountability.

Operation & maintenance stage of a biometric system

Although this diagram just provides several examples of tasks that can be performed at the different stages, it is important to mention that the stages of the lifecycle are quite similar both for video surveillance and biometric systems, except for this stage.

Biometric systems have two modes of operation: **enrolment** and **matching,** and this may require to set up additional mechanisms and procedures for maintaining the integrity and accuracy of the biometric information stored in the system.

- **Retirement**: this is the end of the biometric system life cycle. The system is disposed normally due to business decisions (e.g. replacement of legacy systems) or changes of the stakeholder needs (e.g. the system is no longer required), and its retirement has to be carried out in a controlled manner according to laws and regulations. In the case of biometrics, as for any identity management system, it is important to ensure that all identity information is completely deleted, or otherwise rendered useless when the system is no longer operational.

  A person with technical background should be in charge of the retirement of the system, but it would be also good to include somebody with legal background to verify that the procedure complies with the current legislation.

  Again, the SALT references can provide guidance to facilitate the retirement of the system taking into account privacy and accountability.

We haven't considered *Testing* as a stage itself, as several tests can be conducted during the lifecycle of a system for the evaluation of its performance (e.g. technology testing, scenario testing or operational testing). In this diagram the testing operations are included as tasks carried out in specific stages.

The following table summarizes the SALT resources and includes some examples of knowledge that can be used at each stage of the development process:

Stage	SF Resources	Examples of Knowledge
Concept	• Questionnaires • SALT References & Taxonomies	PIA, Questionnaire, Privacy & Accountability requirements
Design	• Questionnaires • SALT References & Taxonomies • Design Validation Tool	Privacy & Accountability requirements, PETs and technical recommendations
Development	• SALT References & Taxonomies	Recommendations for the use of certain technologies or architectures
Deployment	• SALT References & Taxonomies	Guidelines for system installation, legal requirements
Operation & Maintenance	• SALT References & Taxonomies	Guidelines for the system maintenance
Retirement	• SALT References & Taxonomies	Guidelines to facilitate the correct retirement of the system

4.3.1 **Objectives of guidelines**

The objectives describe what should be achieved by the guidelines when interacting with the SALT framework. The following issues are related to the technical dimension:

- The general process for the design of surveillance systems using the SALT framework, including the steps of the process and when exactly to use the SALT framework.

- How to use the SALT framework to extract useful knowledge and recommendations. The questions include which information has to be provided to the framework, how to use the SALT management tool, and the format of the recommendations obtained.
- How to implement the recommendations including the steps to follow the recommendations, and who should be involved in this process, how to obtain further information in case of doubts.
- How to use the SALT framework to validate the system designed, which information has to be provided to the framework and in which format, how to use the SALT framework management tool for validation.

Thus the guidelines should demonstrate that they can help the user get satisfactory answers during the use of the SALT framework.

4.3.2 Guideline for SALT building process

The SALT building process is focus on the capture and acquisition of SALT knowledge into the framework, using SALT management tools. The guideline specifies the information source and how to input it using SALT management tool.

The information related to video surveillance system includes: surveillance goals, design choice about cameras, network, storage, system management, analysis capabilities, and operator system and procedures.

The information related to biometric system includes biometric system requirements, system characteristics, selection of technologies and sensors, processing units, data transmission and storage.

4.3.3 Guideline for SALT use process

The guideline for video surveillance system should focus on the steps in the development lifecycle, as described in D4.3. That is, how to apply the SALT knowledge at different steps in the development lifecycle.

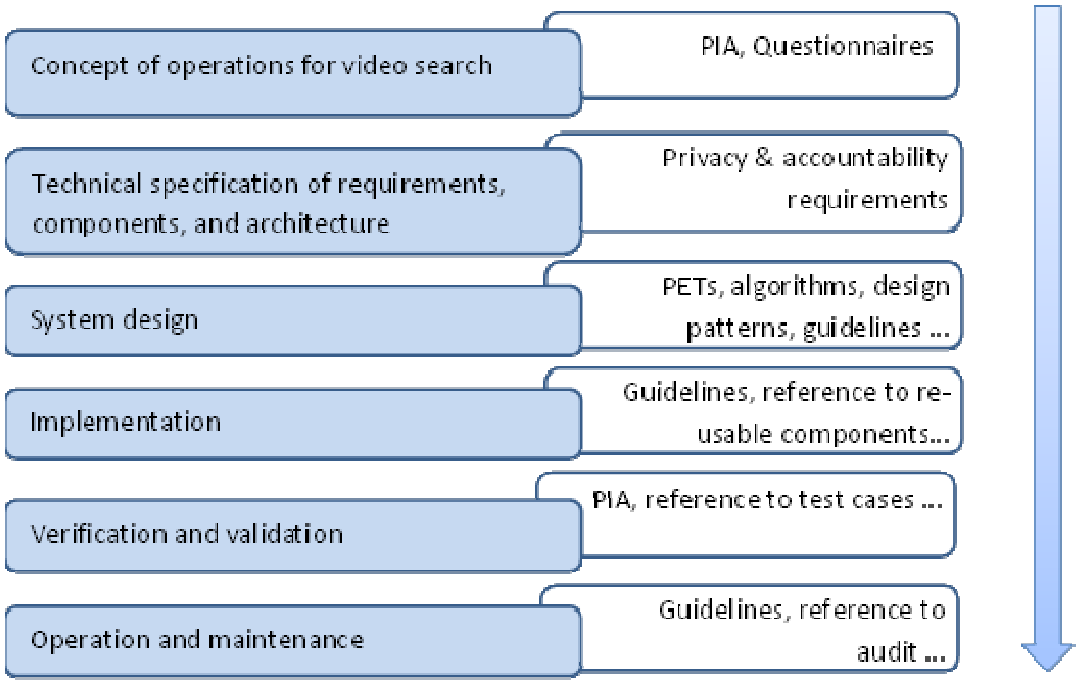


Figure 5 SALT knowledge at different steps of the development cycle

The guideline for biometric system will have the same focus, as described in D4.3, and guides the designer to seek information and knowledge from the SALT framework.

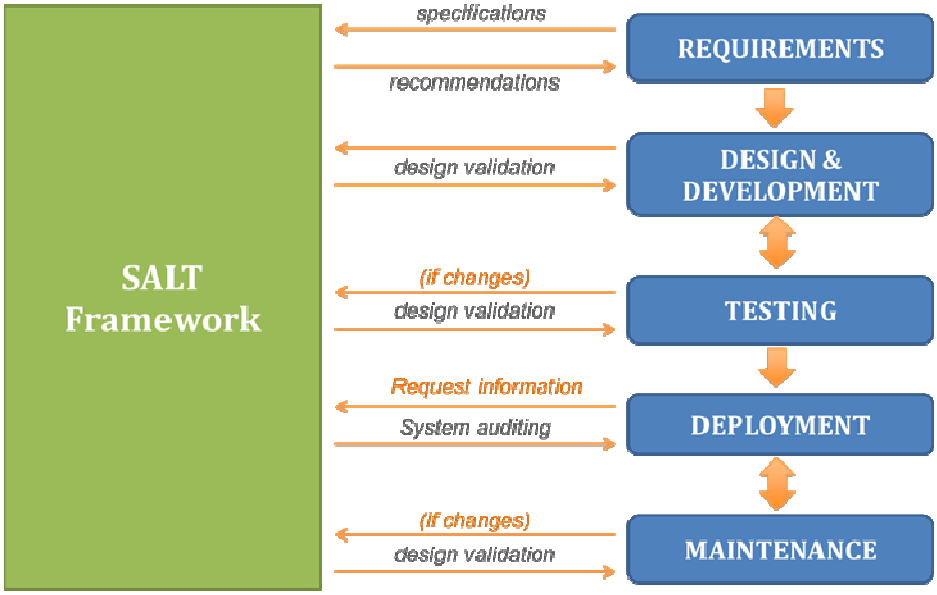


Figure 6 Guideline for SALT use process

4.3.4 A first example: Biometrics guidelines

In the domain of biometrics, there are two main groups of users that will interact with the SALT Framework:

Experts on biometrics, who will provide inputs based on their expertise to the SALT knowledge repository. Their contribution will serve to introduce new references in the SALT Framework

(*create references*) and to adequate the existing ones to the particularities of biometric systems (*update references*).

Biometric systems designers, who are responsible for the design and development of the biometric system based on a set of requirements, provided by service providers and system owners. The system designers interact with the SALT Framework to get recommendations and concerns for the design of a system and to verify that the system created is SALT compliant.

In both cases, the users have a technical profile but do not have to know anything about laws or ethics, so the information related to those fields should be easily understandable by non-experts.

Eventually, other users involved in the lifecycle of biometric systems may require the use of the SALT Framework for auditing purposes (e.g. Data Protection Officers) or to get information about how the SALT Framework can be used to improve a biometric system (e.g. Service Providers).

The guidelines should provide at least information about what the SALT Framework is for, and how to use it for the tasks required by each group of users.

4.3.5 A second example: Video-surveillance technical guidelines

For a video-surveillance system, the SALT user guidelines will mainly cover the 4 following fields of knowledge:

- **How to use the SALT framework to design a video-surveillance system optimized from privacy and accountability points of view.** This body of knowledge and guidelines are typically organized alongside with a typical system engineering process,

- **How to use the SALT knowledge about video-surveillance systems capabilities**. This body of knowledge encompasses the technical capabilities and available performances with respect to the exact technology being used. As an example, considerations about camera performances are part of this knowledge. Most advanced and up-to date information may also enter the knowledge, such as information about smart wearing surveillance capabilities, about drones with onboard imaging sensors, about intelligent glasses are intended to be available,

- **How to use the SALT knowledge to tune the performance of the video-surveillance system according to a context and a mission**. As an example, the technical capabilities and wish-able performance within an international airport, or within a medium size city will be documented, possibly taking into account a risk level,

- **How to use the SALT knowledge to browse the technical harms to privacy and technical mitigations to these harms.** This body of knowledge may e.g. contain information about hardening operator stations, hardening network devices.

4.4 The SALT framework at work or "Integrating dimensions for a domain approach": the example of accountability

The project gave a salient role to the implementation of accountability mechanisms in the design of surveillance systems in order to counterweight the increase in powers given to the owners of such systems. The challenge was to devise the best ways to implement these mechanisms into the design process. The task was not easy as the concept of accountability is multifaceted, depending on which discipline defines its content and its goals. The case of accountability thus turned out to be illustrative of what the SALT framework is meant to achieve: to broaden the limited approach of one discipline to bring the user to adopt a multifaceted solution that integrates the viewpoints of other disciplines.

In the field of surveillance, implementing accountability mechanisms could mean different things depending on which domain perspective the user is looking from. In D.2.3., the goals and meanings of accountability were clarified. Two goals were identified, namely: (1) to ease answerability and (2) to increase verifiability.

Answerability was defined as "the process through which an organization makes a commitment to respond to and balance the needs of stakeholders in its decision-making process and activities and delivers against this commitment".[1] It is concerned with tools that will facilitate engaging with, and being responsive to stakeholders; taking into consideration their needs and views in decision-making; providing an explanation as to why they were or were not taken on board[2]. They refer to the social acceptability of the tools, i.e. its acceptance by the relevant stakeholders. In that sense, these considerations relate more to the ethical viewpoint, but also to the legal perspective in so far as an obligation to consult stakeholders was introduced in the draft General Data Protection Regulation.

Verifiability was defined as the possibility to register the actions and decisions of the surveillance system owners and operators, for further internal or external checks. It is concerned with tools such as the design and implementation of policies, procedures and practices that will aim at ensuring and demonstrating compliance with the commitments and obligations of the surveillance system owner. It is meant to offer validation (compliance with established policies), attribution of responsibility and provision of evidence. These tools relate to the legal domain, in so far as the obligations and the commitments to be verified stem from the legal framework or from contractual obligations, but also to the technical domain that will provide tools to trace the operations performed over the data (thus providing hard evidence).

For these reasons, it was first agreed that the SALT framework would incorporate a dedicated section for accountability under each of the three domains (ethical, legal, technical). The introduction of accountability aspects in the questionnaire developed for WP6 (biometric use case) has further shown that each domain should intervene at a different stage of the process as they aim at different goals. It also showed that they mutually reinforce each other's. By considering all three domains, the user is able to come up with a more complete solution for the requirement of being accountable, i.e. assuming responsibility for the way how personal data are being processed. This also explains why only one aspect of accountability was taken into account for the WP5 use case, the technical domain. Indeed WP5 use case only focused on one part of the process, the design process, which is only affected by the technical approach to accountability.

[1] Mounir Zaharan, Accountability frameworks in the United Nations System, doc JIU/REP/2011/52011,Geneva, 2011.

[2] Monica Blagescu, Lucy de las Casas, Robert Lloyd, "Pathways to accountability, a short guide to the GAP framework", One World Trust (2005).

In this section we recall how each domain approaches accountability, based on the work done in D.2.3., and we explain how the approach of each of three domains (ethical, legal, technical) to accountability are integrated into the WP6 questionnaire that aims at covering the whole PbD process.

4.4.1. Ethical viewpoint: Consultation of stakeholders

From an ethical viewpoint, accountability is approached from its dimension of answerability and intends to foster responsible decision-making. What is important in this regard is to ensure the transparency of the decision-making process towards the relevant stakeholders, their engagement into the process in the form of a dialogue, and the commitment to take their opinion into account and to justify the final decision based on the dialogue engaged.[3] It is argued that in the development of new technologies and services, because of the complexity of the society we live in, no one has an overview of all consequences of a technological development. Many actors have only limited insight into the opportunities and risks involved and restricted means to respond.[4] The engagement of all relevant stakeholders, the clear identification of their responsibilities in the identification of the ethical issues raised by the project combined with the performance of a risk assessment will give legitimacy to the decision-making process towards the use of new surveillance technology.

The tool considered within PARIS to ensure answerability has been the consultation of stakeholders. Stakeholders are individuals and groups that can affect or are affected by an organization's policies and/or actions. They can be internal or external to the organization.

The output has been twofold:

- A series of questions to guide data controllers to organize the consultation of stakeholders, applicable to all surveillance systems. We recommend data controllers to perform the exercise twice:
    - Once the opportunity to deploy the system has been assessed. The consultation here aims at identifying additional privacy concerns that would not have been spotted previously.
    - Once the mitigation measures have been defined in order to check whether stakeholders consider these measures are sufficient.
- A series of recommendations for the processing of biometrics relating to minors and employees and to organize the consultations of these stakeholders. The recommendations are shown to the SALT users at the end of phase 1, if she opts to carry out the consultation.

This section further gives examples of the questions, information and recommendations provided.

[3] See D. Wright (2011), "A framework for the ethical impact assessment of information technology", Ethics Inf Technol, 13, pp. 199–226. The author identifies accountability only with the distribution of responsibilities among the different stakeholders. However, if we approach accountability as a process, the concept should extend to include the process of engaging and consulting stakeholder to ensure ethical issues are identified (transparency), and of engaging into the performance of a risk assessment. This approach is coherent with other accountability frameworks, e.g. the Global Accountability Framework developed by One World Trust (see PARIS Deliverable D.2.1., p. 140 and following).

[4] Ibid.

Organizing the consultation of stakeholders

A series of questions were drafted in order to guide SALT users when deciding how to consult stakeholders. They review the different considerations that should be taken into account depending on the level of engagement of these stakeholders into the process that has been decided. These questions are applicable to the design of all systems. They are not specific to the WP6 use case.

Before accessing the questions and in addition to the explanation contained in the questions, SALT users are given this general information about the content and purposes of the section on stakeholders' consultation. We have taken into account that SALT users can have different profiles, thus different needs, as identified in D.2.3.

Information provided as introduction

In order to fully define the context of the personal data processing activity, it is necessary to identify its implications and expected benefits for the entity but also for individuals and organisations impacted by the processing, be it citizens or technology providers. Under Art. 32.4 of the Draft General Data Protection Regulation, the consultation of data subjects or their representatives would become a legal obligation.

This means opening channels of participation but also implementing a process to take these concerns into account and inform stakeholders about the results of the consultation process, explaining why certain concerns were taken into account while other were discarded. This consultation process is time consuming but it is crucial to obtain the views of people or entities not directly involved in the project, thus able to provide a broader perspective. It can serve to highlight risks that were not spotted in the first place.

The consultation process enhances the transparency of the organization and of the project. It allows the organization to make a commitment to respond to and balance the needs of stakeholders in its decision-making processes and activities and delivers against this commitment. It is a process for learning. The ultimate goal of consultations is to generate ownership of decisions and projects and to enhance the sustainability of activities.

If the organization decides to engage towards a proactive approach and becomes accountable to its stakeholders, the organization One World Trust has for instance developed an accountability framework to provide guidance to organizations on how to operationalize accountability. Five dimensions should be taken into account when designing accountability mechanisms: drafting an accountability strategy, transparency, participation, evaluation, and complaint and response mechanisms. More information can be found here.

The goal of this section is less ambitious. It aims to help the user to identify the stakeholders who should be consulted and suggest ways to organize the consultation and to integrate the views to the decision-making process (the PIA). To that end it guides the user through an open questionnaire.

When should this consultation process be carried out? As general recommendation, it is recommended to carry out the consultation process once the opportunity to design the system has been assessed and before the mitigation measures are decided upon. The consultation process fully participates from the definition of the risks inherent to the data processing activity. A second round of consultation could occur after the options for the design system

have been taken in order to check to what extent they meet users' concerns.

Example of questions

Who are the persons or groups that can affect or be affected by the surveillance system you intend to deploy?

1. **Goal of the question**: Make the organization aware of who its stakeholders are for this data processing activity and which types of commitments the organization have towards them.

2. **Information associated with the question**: Identifying who your stakeholders are is the first step in having a clear view on which commitments and obligations the organization should comply with. It is also the first step in understanding the different expectations these stakeholders might have and the different forms of responsiveness and accountability which can be inferred from these relationships.

   Stakeholders are individuals and groups that can affect or are affected by an organization's policies and/or actions. Stakeholders can be internal to the organization (e.g. employees, shareholders) or external to the organization (individuals or groups who are affected by an organisations' decisions and activities but who are not formally part of the organization – e.g. data subjects, parents of the minors whose data are processed, contractors).

   Stakeholders have different capacity (resources, knowledge and expertise), different degrees of access to reliable information and different needs and expectations.

3. **Best practice:** The organization One World Trust has for instance developed an accountability framework to provide guidance to organizations on how to operationalize accountability. Five dimensions should be taken into account when designing accountability mechanisms: drafting an accountability strategy, transparency, participation, evaluation, and complaint and response mechanisms. More information can be found **here**.

Recommendations

The WP6 questionnaire contains high level recommendations to carry out the consultation of two types of stakeholders, who are more likely to be affected by the use of biometrics for access control purposes: minors and employees.

We considered that in order for the consultation to be meaningful, the consultation should first occur once the decision had been made to go on with the development of the system. This first round of consultations is meant as "reality check" to verify that the surveillance system could be acceptable for data subjects that will be monitored by the system and to spot additional concerns not initially taken into consideration which could either lead to the abandon of the system or to impact its design.

Example

1. **Identify the relevant stakeholders of the information system that will process children's biometric data.**
   a. In addition to children and their legal representatives (e.g., parents or legal

guardians), there are other people who could be present in the environment of the system and who may be affected by the system. For example, in situations where a biometric system would be used to facilitate the borrowing of library books, librarians could be included in the consultation, whereas in situations, where a biometric system would be used to speed up the management of payments for a meal at a canteen, canteen workers could be consulted.

b. To ensure that best interests of children are considered, it is recommended to consult a wide range of stakeholders (e.g., children, their legal representatives, teachers, librarians, canteen workers, and the parent council) who may be directly or indirectly affected by the system.

4.4.2. Legal viewpoint: Internal privacy policy

From a legal viewpoint, accountability is approached as a tool to promote legal compliance. An accountable organization is expected to ensure and demonstrate compliance with the legal framework. Thus, accountability entails no more than an assumption and acknowledgement of responsibility and an obligation to demonstrate compliance upon request to the competent supervisory authority.

Accountability is therefore concerned with the design and implementation of policies, procedures and practices that will aim at ensuring and demonstrating legal compliance. The outcome of the accountability mechanisms should serve to demonstrate the entity abides by the applicable legal framework.

Recommendations for accountability mechanisms directed to policies aim both at defining the commitments of the entity in terms of privacy both internally (personal data management, creation of new products and services) and externally towards data subjects. In the latter case, the key idea is to increase transparency of data processing activities to individuals. SALT experts can be most helpful by pointing out which types of information are to be given to individuals and how to display this information, for example through the indication of best practices. This will relate for instance to the types of data processed, purposes of the processing or communication channels enabled.

Recommendations for accountability mechanisms directed to procedures will relate to organizational measures implemented by the entity to ensure that policies are implemented in practice. They are concerned with initiatives such as privacy management programs.

Recommendations for accountability mechanisms directed to practices will be concerned with the description of the kind of evidence that should be available at the level of systems so that compliance can be checked with regards to technical rules stemming from privacy requirements. This evidence concerns both general features of the system, such as the employed security or cryptography mechanisms, and the actual executions runs of the system. This is dealt with in the technical viewpoint section.

The tool considered under PARIS to help data controllers complying with their obligation to demonstrate compliance with the legal framework has been the drafting of an internal privacy policy, i.e. to specify the rules and procedures that should apply internally to the personal data processing activities.

The output has been twofold:

- Guidelines for the drafting of an internal privacy policy
- Specific questions directed to ensure the accountability of the data controllers inserted in the WP6 questionnaire.

Guidelines to draft an internal privacy policy

Before accessing the questions and in addition to the explanation contained in the questions, SALT users are given general information about the content and purpose of the guidelines.

Information provided as introduction

The purpose is to guide the user in order to define an internal privacy policy that includes policies and procedures regulating a given personal data processing activity. It takes the user throughout the different elements that an internal privacy policy should contain and provides explanations about the expected content of each section.

The concept of this questionnaire is based upon set criteria, detailed in the following seven categories:

1. Purpose of the processing
2. Data collection (inventory)
3. Data accuracy
4. Data use and disclosure
5. Security
6. Rights of the data subjects
7. Governance structure

The following questionnaire is designed to provide a starting point to conduct an in-house privacy assessment and brief descriptions of key point notions are provided in each category.

Examples of the information provided under a sub-section: ensuring compliance of the data processing activity with its purpose

1) Purpose of the processing

Each processing of personal data should have a clear, explicit and specified purpose. Processing of personal data refers to 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.

This means that the purpose should be defined before data are collected and, wherever relevant, data subjects should be informed of this purpose. The purpose should also be legitimate, in other words, the data processing activity should have a clear legal basis, i.e. the data processing activity should be based on one of the grounds listed by the 95/46/EC Directive (the Data Protection Directive)

The definition of the purpose is paramount as it will have an impact on several aspects of the data processing activities:

- Data collection: only data that are strictly necessary for the purpose of the processing must be collected. (see section 2)
- Data processing: the personal data processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. This obligation applies not only to the data collection phase but also throughout the processing. (see section 3)
- Further uses: Personal data should not be further processed in a way incompatible with the original purposes of collection. (Section 4).

It is thus paramount to clearly define the purpose of the data processing activity and ensure they adequately reflect the intentions of the data controller.

Questions	
1. What is the purpose of the processing?	
2. On which legal basis does the processing rely on?	

Questions included in WP6 questionnaire

☐ The individuals is provided with the necessary information in order to understand fully the reasons and implications of being enrolled in the biometric system

Explanation: *The data controller should Ensure that individuals to be enrolled in the system receives sufficient information about the purposes and modalities of the system, as well as about their rights to ask for access and deletion of their data.*

Data subjects must be informed about the data processing activity and its purposes before or at the time their data are collected (Directive 95/46/EC Articles 10 & 11). The information notice that is communicated to data subject during the enrolment phase should contain the following items:

- *a description or visualisation of the matching procedure during which extracted bodyprints allow to identify a person (Biometrics Constitution);*
- *the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;*
- *the purposes of the processing for which the personal data are intended;*
- *the period for which the personal data will be stored;*
- *the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;*
- *in cases, where consent is required, provide a possibility to withdraw it;*
- *the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;*
- *the recipients or categories of recipients of the personal data, and conditions under which data may be transferred to the recipients (e.g., access to a video may be provided upon an official request of a*

law enforcement agency);

- *where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;*
- *any further information necessary to guarantee fair processing in respect of the data subject (e.g., the procedure for the repudiation, under which conditions reenrolment procedure has to be repeated), having regard to the specific circumstances in which the personal data are collected;*

the level of security during all processing stages including transmission (e.g., over networks).

4.4.3. Technical viewpoint

From a technical viewpoint, accountability will be envisaged as aiming at defining data handling policies, specifying the design of processing evidence in execution traces called logs and implementing automatic a posteriori compliance checking mechanisms between policies and logs. Accountability in the technical sense of the term is a property of a data processing system. As such, accountability offers three capabilities:

- Validation (checking log compliance with respect to policies), which allows users, operators and third parties to verify a posteriori if the system has behaved as expected (in line with previous agreements over permissible data handling) over the entire lifecycle of personal data;
- Attribution (allocating responsibilities): in case of deviation from the expected behaviour (fault), revealing which entity is responsible and under which circumstances;
- Provision of evidence: the generation of evidence that can be used to convince a third party that a fault has or has not occurred.

Questions and recommendations contained in the SALT framework focus on the nature of relevant evidence to facilitate the compliance checking process.

The output of the technical accountability requirements are twofold:

- Specific questions directed to ensure that technical accountability is taken into account by the designers (and that justifications are provided if certain recommendations are not followed)
- Integration of accountability requirements in the design of the system itself (accountability by design)

As an illustration, a key accountability requirement is the possibility to control and trace any access to personal data and their deletion, which is expressed through the following sections of the questionnaire:

1. Which entity has access to the biometric data? Under which conditions?

Response

The System Administrator has access to the biometric data for enrolment, or to update an inaccurate biometric template.

Besides, any data subject will be able to request access to their personal information stored in the system. This access will be authorized, traced and supervised by the System Administrator.

2. Can data be transferred to third parties? Under which conditions?

Response

In case of detection of an unauthorized access to the office, the incident will be reported to the local authorities and the relevant data can be transferred to the police for the purposes of the investigation and prosecution of the unauthorized person.

Under no circumstances, the Data Controller will share the information stored in the system with the security company contracted for the security alarm service, or with the maintenance company.

3. Are they automated data erasure mechanisms in place to ensure that biometric data will not be stored for longer than necessary?

In order to prevent that biometric information are stored for longer than is necessary for the purposes for which they were collected or subsequently processed, appropriate automated data erasure mechanisms have to be implemented also in case the retention period may be lawfully extended, assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system.

When using integrated storage on the reader, manufacturers may also implement storage of the biometric templates on volatile memory that guarantees that the data will be erased when the reader is unplugged. Therefore no biometric database remains when the reader is sold or uninstalled. Anti-pulling switches may also be used to automatically erase the data if someone tries to steal the reader.

Response

DELETION PROCEDURES

RGB and depth images (videos):

- During the enrolment, the videos captured have to be deleted manually by the System Administrator once they have been analyzed and the most adequate bodyprints have been selected for the person to enrol.
- In the matching phase, the video frames are automatically deleted by the system right after the bodyprints have been extracted. Besides, each time a VPU is switched on for matching, all the temporary storages containing images and bodyprints are automatically cleared.

Bodyprints extracted for enrolment:

- The bodyprints discarded are deleted automatically after selecting the bodyprints that will be stored in the template database. This task is performed through the Enrolment User Interface.
- The bodyprints composing the Authorized People Database (APDB) are kept in the system until the person is unenrolled, or the system is retired, or until they are replaced by more accurate bodyprints from the same person.

New Bodyprints extracted during the matching phase:

- In the VPUs, the bodyprints have to be first marked by the RIS as “collected”. A scheduled process in each VPU will periodically review the bodyprints and will delete those marked as “collected”. Besides, each time a VPU is switched on for matching, all the temporary storages

containing images and bodyprints are automatically cleared.

- In the RIS, the new bodyprints collected for matching are deleted automatically right after the comparison has been performed.

Key frames:

- During the enrolment, only the key frames of the selected bodyprints are kept, the other key frames are deleted after selecting the bodyprints that will be stored in the template database.
- The key frames stored with the bodyprints of the APDB, are kept until the person is unenrolled, or the system is retired.
- During the matching phase, the key frames are kept until the results of the comparison are reviewed by the System Operator. All the key frames of events corresponding to authorized accesses will be automatically deleted after the revision. On the other hand, the key frames of events related to intrusions or suspicious accesses, will be kept in the system until the incidents are resolved.

  In any case, the key frames are encrypted and can only be decrypted by a user with administrator or operator privileges.

Finally, out of the detection period, the biometric system will be switched off.

As far as the design of the system is concerned, a key recommendation is to register evidence about data handling in the form of system logs. Although the use of logs was already foreseen, the recommendation led the *System Designer* to refine the information that should be included in the different logs and the process and operations to be traced. In order to register who has access to the information stored in the system, the main resources of each component implement access control mechanisms (e.g. interfaces, web services, databases). Besides, these user profiles were defined at the design stage with different permissions to access the system resources. Another recommendation is to use log analyzers that can automatically verify the compliance of the system operation with the declared privacy policies. However, the *System Designer* decided to perform this task manually if necessary due to resource restrictions. On the organizational side, it has also been required that, for accountability purposes, the *Installer* shall sign a document including details of the installation conducted.

5 Conclusions

This document provided guidelines for SALT users, i.e. the people in charge of applying the SALT frameworks and constitutes an update of the D2.3 Guidelines. The introduction explained how the deliverable has been framed, what are its purposes and what it intends to realize, i.e. facilitating the appropriation and use of SALT frameworks by SALT users. To do that, it first grounds the "Guidelines for users" in a "domain approach" (1.2) and explain the main inputs and outputs of the guidelines for users (1.2), assuming that the most relevant entry point to SALT framework depends upon the user's desired level of expertise.

The section 2, "Concepts of SALT frameworks for users" was an introduction to the main concepts used in the SALT framework in an easy and understandable way, so that SALT users may easily apprehend what SALT frameworks are about, what they deal with and what they encompass. It started by recalling the approach decided upon in D2.2., namely a questionnaire-based approach to cope with legal, socio-contextual and ethical, technical and accountability dimensions (2.1). Then it recalled the three-stage process, i.e. that SALT systems are put into place sequentially. In this respect, we identified three stages of development of a surveillance system: conception, design and implementation (2.2). Lastly, it introduced the guidelines and their definition, their purpose, and the extent to which they will be useful for SALT users (2.3).

Section 3 & 4 were dedicated to the guidelines for users of SALT frameworks. Section 3 presented the guidelines for creators of references, namely the SALT experts. Although PARIS partners have agreed about a common template (3.1), specific guidelines have been addressed for each category of references, namely for socio-ethical and contextual references (3.2), legal references (3.3), and technical references (3.4).

Section 4 introduced the guidelines domain by domain. First, it dealt with the socio-contextual and ethical dimensions, and suggested a certain amount of guiding principles to apply SALT frameworks under these dimensions (4.1). Second, it addressed the legal dimensions of SALT processes and explained how to integrate certain fundamental legal notions such as privacy, data protection, or yet the principle of proportionality among others (4.2). Third, it dealt with the technical dimensions and identified the relevant technical users and provided step-by-step guidelines that will take him/her through the development process (4.3). Lastly, we examined the accountability dimension (4.4). This dimension crosscuts many aspects of both the socio-contextual and ethical, legal and technical dimensions.

In addition to the "Guidelines for users", this report further contains five annexes, gathering all the contributions prepared by the main partners involved in the definition of a SALT framework in relation to biometric systems. Indeed, as suggested in D2.1 and D2.2, a specific research has been carried out in order to prepare a SALT questionnaire for biometric systems of authentication. The SALT biometric questionnaire aims at providing appropriate assistance to decision-makers regarding the conception, design and implementation of a biometric system. Altogether, these five annexes summarizes the research carried out during the last period of PARIS project and constitute a concrete illustration of the application of the concepts described in section 2 and the guidelines and principles explained in section 4 of the deliverable.

More specifically, Annex 1 constitutes an introduction to the biometric questionnaire and explains the methodology applied for the selection of the criteria to be taken into account in order to assess the proportionality of a biometric system in a first stage. This research has included an extensive study of the French caselaw in relation to biometric systems, contributions from the Council of Europe, the Working Party 29 and literature. Annex 2 contains the final draft of the biometric questionnaire aiming at assessing the "opportunity" of

a biometric system in the light of the criteria of purpose, legitimacy and necessity. Annex 3 is dedicated to the issue of consultation of stakeholders and how such consultation is included in the SALT questionnaire through questions and specific recommendations according to the categories of people enrolled in the system. Annex 4 deals with the “Design” phase and includes all the questions that should be addressed step-by-step by systems designers and system owners when designing a biometric system. Annex 5 relates to the third phase of the questionnaire “final balancing” and Annex 6 deals with the issue of governance, providing guidelines to draft an internal privacy policy for the management of the biometric system installed.

Annex 1. Balancing privacy and security in the case of biometrics: introduction to the biometric questionnaire

1.1 Introduction

As explained in previous report, especially in D2.1 and D2.2, we suggested carrying out a specific research in order to propose a specific questionnaire (presently non-existing) in the field of biometrics as biometrics was one of the case study. Biometrics was selected as a potential case study to implement the principles, approach and methodology defined in section 2 of the present deliverable. We selected biometrics instead of video surveillance in view of the absence of specific legislation, at European and national level, and important need to provide guidance to system owners and system designers on this issue.

1.1.1 **Structure of the questionnaire**

The structure of the questionnaire that has been prepared focuses on two sections: Opportunity and Design. The major contribution and innovation in the questionnaire that has been created relies on its dynamic character. Certain criteria have been identified as essential « proportionality criteria » helping the decision-maker to assess the overall impact of his biometric project on privacy and data protection rights. The dynamic dimension of the questionnaire has been introduced in the first stage, called « opportunity », the goal being to provide an assessment of the project to the user. The second stage dedicated to the « design » of the system aims at accompanying the user in taking into account data protection requirements.

1.1.2 **Scope of the questionnaire**

The questionnaire addresses the deployment of biometric systems in the private sector. The use of biometrics in the field of law enforcement, forensics or national identification requires the intervention of the legislator. This implies that specific debate will generally occur in order to address the balance between privacy and surveillance. Instead, the deployment of biometrics in the private sector is not specifically foreseen in most EU Member States and system owners or system designers have to interpret and apply the general data protection legislations to their biometric system with little, if any guidance from EU Data Protection Authorities. Besides, the issue of the balance between fundamental rights and surveillance is substantially different in the public or private sector. We decided to focus on the private sector.

1.1.3 **A twofold dimension**

As explained in the D2.1, D2.2 and D2.3, the challenge of the questionnaire is to operationalize the principle of proportionality, which is a condition for a lawful interference into individual's right to privacy, in view to accompany the decision-making process regarding a surveillance system. The first part of the questionnaire combines two complementary dimensions.

1.1.1.1 The reflexive dimension

First of all, the questionnaire carried *a reflexive dimension:* under this dimension, the user is requested to answer to some open questions, accompanied with appropriate information/explanation destined to help him to determine his/her needs for a biometric system and identify potential less intrusive alternatives. The major well-known conditions set

by the principle of proportionality have been taken into account in order to stimulate a reflexive approach among the decision-makers. As explained in the D2.2, this objective is pursued with open questions, built on the permissible limitation test proposed by P. De Hert in view to assess the impacts of a new surveillance technology on private life from a Human rights perspective[5] and on the very well know three stages process of the proportionality principle. For the record, the proportionality test involves a three-steps analysis: i) the suitability stage, that is to say whether the interference is appropriate in that it effectively achieves the aim pursued; ii) the least-restrictive means test or subsidiary principle, or whether the State could have achieved the legitimate aim pursued with a less restrictive measure for the fundamental right at stake; iii) the balancing test *stricto sensu*, which *in concreto* balance the interests in presence.[6]

Basically, the questions retained question the surveillance needs (Q.1 What is/are the purposes of the biometric system?), the suitability and effectiveness of a biometric system in relation to the needs (Q. 6, Is there evidence that the intended surveillance system have produced, in similar other cases or circumstances, the expected effects?), and questions regarding potential less intrusive alternatives (Have other means, in particular non-technological means, been considered to achieve the legitimate stated objective(s)? If yes, which are they? Are these means less intrusive or could they be considered as less intrusive? Why have these means been put aside? Why do you believe that the intended surveillance system is the less intrusive mean to achieve the legitimate stated objective(s)?).

1.1.1.2 The evaluation dimension

Most importantly, this first part of the questionnaire brings *an evaluation dimension*: under this approach the questionnaire tries to evaluate the overall proportionality of a biometric system on the basis of a limited number of essential criteria. This is where the questionnaire intends to provide an automated impact evaluation of a biometric system. Such an approach is very innovative, since it remains widely unfamiliar to lawyers. It is the purpose of this report to explain how those criteria have been identified and selected and to which extent they may provide a useful preliminary privacy impact assessment of a biometric system. We will explain why and how France's policy in this respect has been extensively analysed and used as a relevant case study for the identification of potential European criteria (1). We will then explain which criteria have been retained for the purposes of our privacy impact evaluation (2).

1.2 Background research: the case study of France

As explained in previous reports, especially the D2.1 and D2.2, there is no single, uniform and harmonized interpretation at European level as to which surveillance technology is acceptable or not, and the conditions under which they can/should be deployed. If The Working Party 29 provides some general guidance at EU level (WP193), the D2.1 highlighted the differences of approach between Belgium and France regarding biometrics. While only general guidance is available in Belgium, extensive deliberations have been issued by the CNIL in France regarding biometrics applications. Since 2005, the CNIL is empowered to authorize biometric systems

[5] Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in *Privacy Impact Assessment,* ed. David Wright and Paul de Hert, (London, Brussels, Springer: 2012), 33-76

[6] The said definition of the content of the proportionality principle derives from Robert Alexy, *A theory of Constitutional Rights*, trans. Julian Rivers (Oxford: Oxford University Press, 2002) (original publication in German in 1983)

(except those deployed following the adoption of decree), and all decisions are publicly available on *Légifrance*. These decisions translate CNIL's proportionality policy in this respect. In that context, CNILS' decisions with respect to biometric systems constitute a very relevant case study providing an important research material in view to identify the underlying requirements taken into account by a Data Protection Authority in the course of the authorization-making process. The goal of this research has of course been to identify these criteria and potentially take them as a source of inspiration for building up our own evaluation criteria.

In France, the processing of biometric data is specifically foreseen in the Information Technology and Civil Liberties Act.[7] Biometric applications carried out by the State for the identification or verification of identity of individuals must be authorized by Decree after consultation of the CNIL.[8] Other "*automatic processing comprising biometric data necessary for the verification of an individual's identity*" are submitted to the prior authorization of the CNIL.[9] The scope of our study was precisely to address this second category of biometric systems, leaving aside the deployment of biometric systems by the State, which are subject to the adoption of a Decree. Instead, we focused specifically on all other situations, which covers in practice all biometric identification carried in the private sector understood widely (including public institutions or public services, as far as they cannot be considered as acting in the course of a public State mission).

In practice, the CNIL has developed a doctrine distinguishing between two categories of processing of biometrics data: a limited list of processing of biometric data is submitted to a simplified declaration, while all other processing remain subject to prior examination and authorization of the CNIL.

The CNIL has adopted 'unique authorization' for a series of processing of biometric data, which are therefore only submitted to a 'simplified declaration' to the CNIL. This is the case for the following biometric systems:

- use of hand geometry to control access to work premises and mass catering[10]
- use of fingerprinting exclusively stored in a personal device to control access to professional premises[11]
- use of hand geometry to control access to school restaurants[12]
- use of vein pattern recognition to control access to professional premises[13]

[7] Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties – Loi No. 78-17 Informatique et Libertés du 6 Janvier 1978 – as amended

[8] Article 27§2 of the Information Technology and Civil Liberties Act

[9] Article 25§8 of the Information Technology and Civil Liberties Act

[10] Autorisation unique AU-007 - Délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail

[11] Autorisation unique AU-008 - Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

[12] Autorisation unique n° AU-009 - Délibération n°2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire

[13] Autorisation unique n° AU-019 - Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

- use of fingerprinting in professional laptops.[14]

	Purposes of processing of biometric data			
Type of biometrics technology	**Access control employees/visitors in professional premises**	**Access control to professional computers**	**Access control to school restaurants**	**Other**
Hand geometry	Simplified Declaration (If compliance with AU-007)	Special prior authorization required	Simplified declaration (If compliance with AU-009)	Special prior authorization required
Fingerprinting	Simplified Declaration (If compliance with AU-008)	Simplified Declaration (If compliance with AU-027)	Special prior authorization required	Special prior authorization required
Vein pattern recognition	Simplified Declaration (If compliance with AU-019)	Special prior authorization required	Special prior authorization required	Special prior authorization required
Other	Special prior authorization required	Special prior authorization required	Special prior authorization required	Special prior authorization required

Table 6: CNIL's categories of biometric processing

This implies that for the situations mentioned in green in the table, the use of biometric technology has been considered as proportionate by the CNIL, provided these uses also satisfy other data protection requirements, such as security requirements. All other biometric applications are submitted to the prior special authorization of the CNIL.

In total, about 4850 biometric systems have been notified to the CNIL between 2005 and 2014.[15] About 4400 concern simple declarations and 458 special decisions, among which 101 systems have been refused, an average of about 2% only.

[14] Autorisation unique n° AU-027 - Délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels

[15] This figure derives from the figures published by the CNIL in its Annual Reports over the period 2005-2014 and from the Report of Senator François Pillet to the Senate of 16 April 2014, available here: http://www.senat.fr/rap/l13-465/l13-465.html (last accessed 30/11/2015)

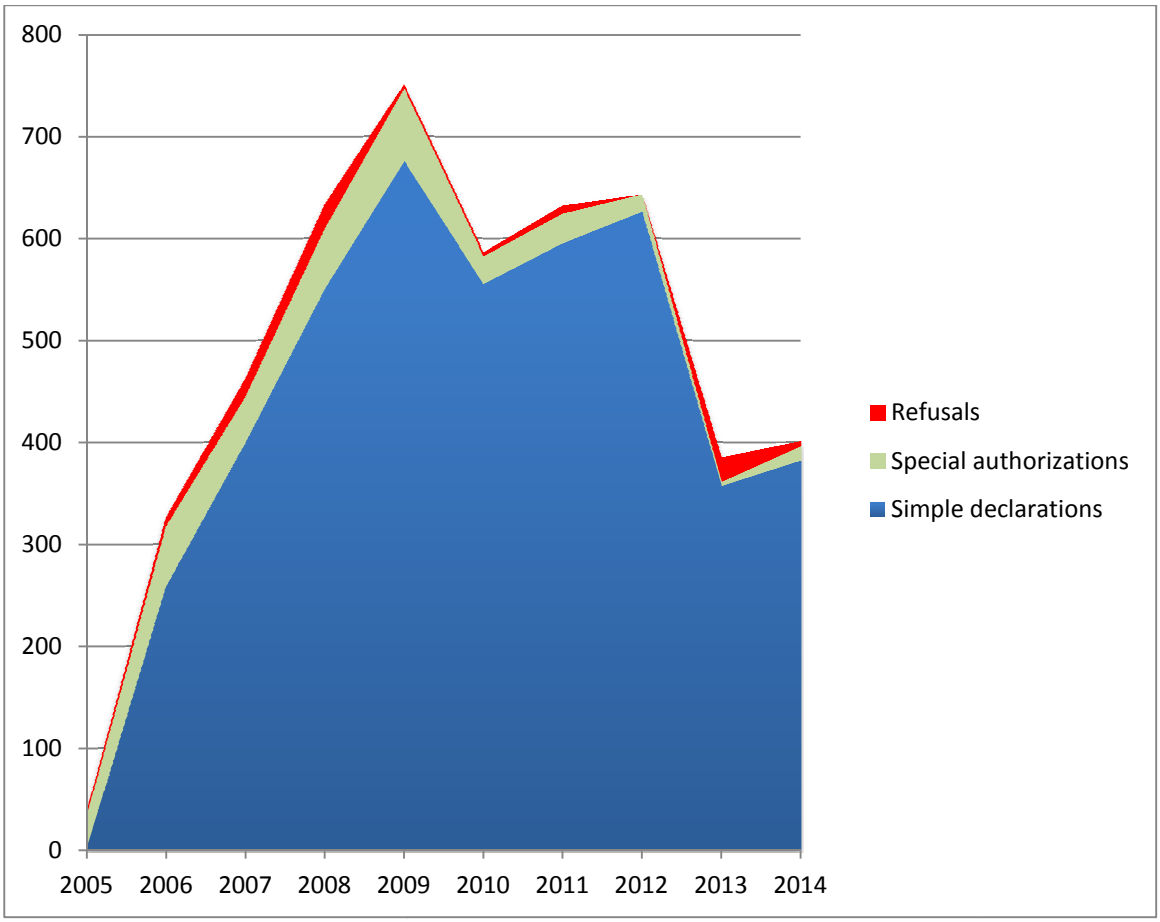


Figure 7 Evolution of Declarations, Authorizations and Refusals of biometric systems in France from 2005 to 2014

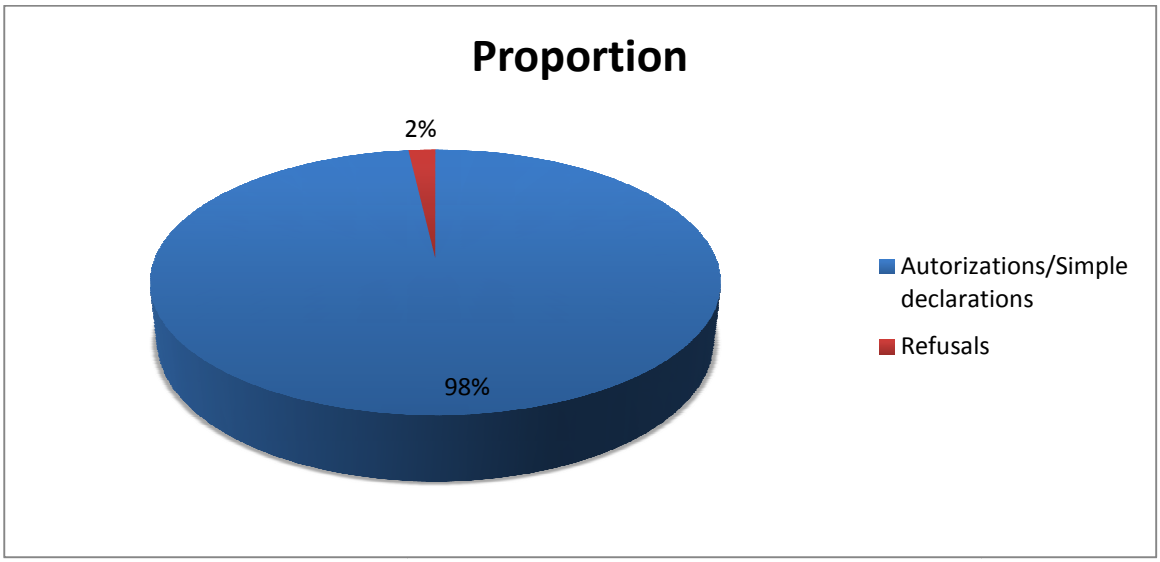


Figure 8 Proportion of Authorizations and refusals of biometric systems in France from 2005 to 2014

The work environment is indisputably the context where biometrics is the most expanded (≈ 84% of biometric systems)[16], followed by schools (≈ 15%)[17], and the use of biometrics for research or experimental purposes (≈ 1%). The use of biometrics in the commercial environment or for other purposes represent less than 1% of biometric systems in France.

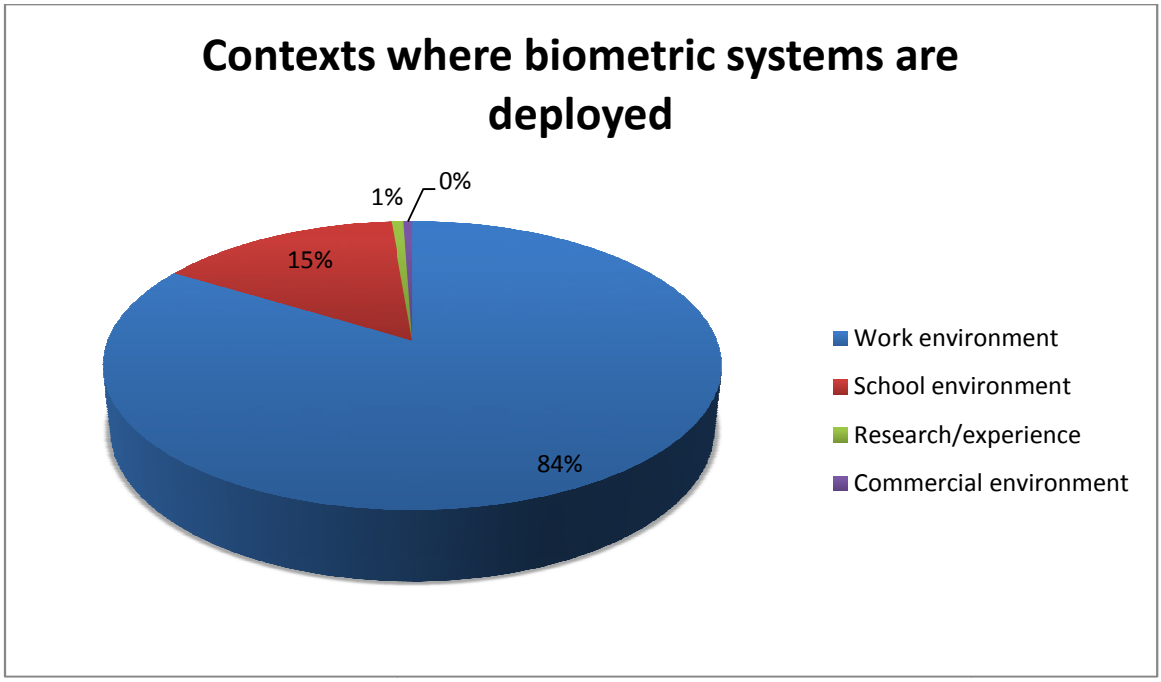


Figure 9 Contexts where biometric systems are deployed in France in the period 2005-2014

[16] The proportion of biometric systems in the work environment is estimated on the basis of the number of simple declarations (All declarations relate to the work environment except AU-009) and special deliberations (special authorizations and refusals) concerning the enrolment of employees.

[17] In its 2010 Annual Report, the CNIL mentions that about 400 biometric systems have been notified to the CNIL in accordance with the Authorisation unique AU-009 (adopted in 2006) for access control to school catering, an average of 100 declarations per year. No other figures have been published further. For the purpose of our estimation, we have raised this number up to 800 (following the average of 100 declarations per year).

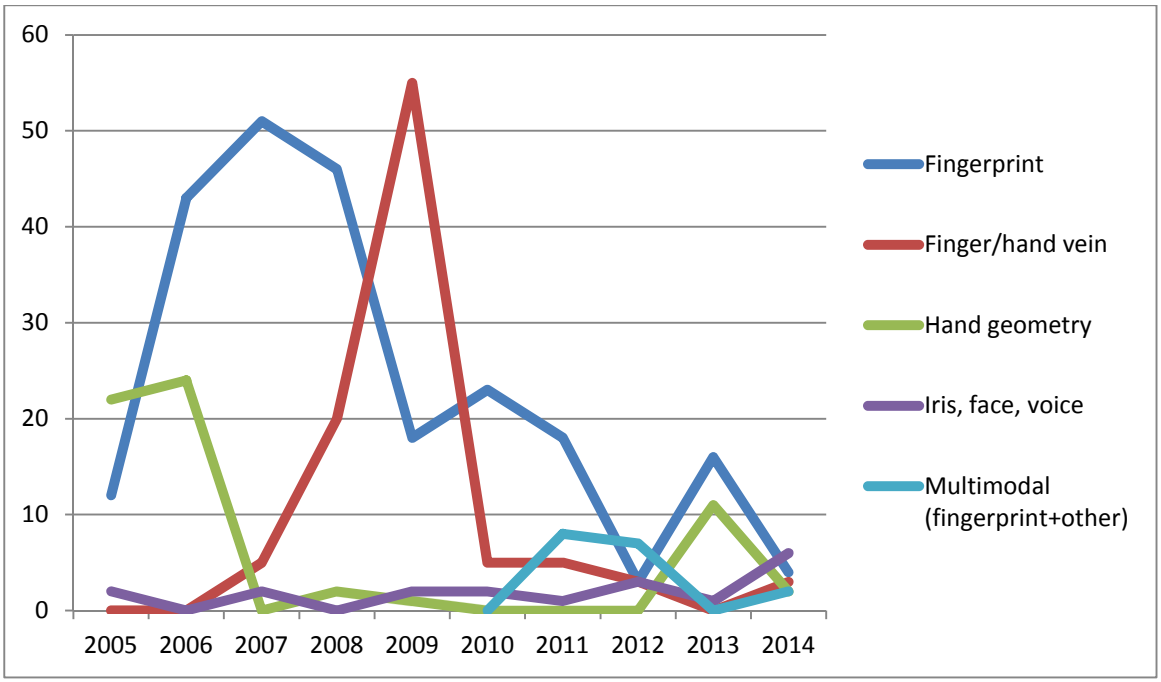


Figure 10 Evolution of types of biometric systems in France in the period 2005-2014

We have conducted a thorough selection and analysis of 458 deliberations (comprising both authorizations and refusals) of the CNIL, delivered in compliance with its power of special authorization within the period 2005-2014 (10 years).[18] The proportion of special deliberations relating to these different contexts and uses also confirm that employers are the most requesting special authorizations (363 special decisions), followed by the research field (41 decisions) and service providers/commercial sites (29 decisions). Only a few deliberations relate to schools (16), showing that other uses of biometrics outside the conditions authorized by AU-009 are not developed. Finally, a small number of decisions (9) relate to other contexts or populations, including students or vulnerable people.

[18] All these deliberations have been classified according to some pre-defined essential context-related information and characteristics of the systems: i) date of the decision; ii) authorisation or refusal; iii) activity of the requesting entity (such as “laboratory”, “casino”, “hospital/health establishment”, “industry/fabrics”, “other private firms”, “firms in the field of surveillance/security technology”, “association”, “school establishment”, “banking/financial sector” and “other”); iv) categories of people enrolled in the system (“minors”, “employees/habilitated persons”, “customers/users of public services”, “patients”, “volunteers”, “vulnerable people”, “students”, “other”; v) type of system (“simple” or “multimodal”); vi) type of biometric characteristics collected (“fingerprint”, “finger vein”, “palm vein”, “palm print”, “iris”, “voice”, “DNA”, “face recognition”); vii) purposes pursued (“identity fraud”, “general security”, “access control to applications/devices/”, “access control to restricted area”, “other”); viii) legal basis invoked (“consent”, legitimate interests of the controller”); ix) place of storage of the biometric data (“individual device”, “terminal/reader”, “central strorage/server”)

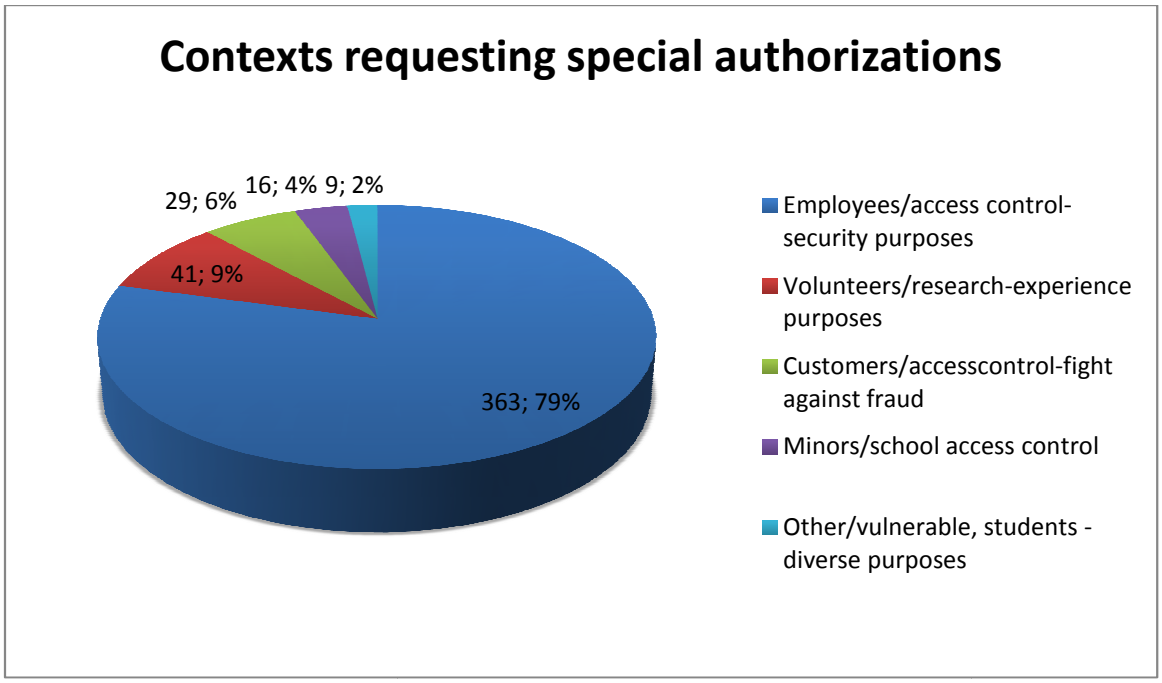


Figure 11 Contexts where specific authorizations of biometric systems are requested in France in the period 2005-2014

The results of this research have been submitted and accepted for publication in an law journal in the field of law & technology.[19] This is why the results presented hereunder are limited to our main findings and conclusions and do not include the whole analysis carried out.

1.2.1 CNIL's criteria of proportionality

From 2005 to 2013, CNIL's methodology for the evaluation of biometric systems was said to be based on the following criteria:

i) the distinction between "pressing security need" requiring the securization of a delimited area representing a "*major stake which surpasses the sole interest of the organization*" and general securization goal or identity management purposes; Indeed, in case of "pressing security need"

ii) the distinction between biometric data leaving trace and biometric data leaving no trace; and

iii) the place of storage of the biometric data, distinguishing the central storage on a server or in the reader and the storage on an individual device.

Another criterion, which is not formally expressed, relate in our view to the categories of persons enrolled in biometric systems and legitimate basis associated to the processing of their biometric data. CNIL's approach indeed distinguishes mainly three categories of people/legitimate basis:

i) the enrolment of employees in biometric systems relying on the legitimate interests of the organization (generally security-related purposes, whether "pressing security " situations or more "general security" contexts);

[19] The results of this research shall be published under the following reference: Claire Gayrel, "The principle of proportionality applied to biometrics in France, ten years of CNIL's deliberations", in *Computer Law and Security Review* (paper accepted), to be published in 2016

ii) the enrolment of minors (generally for identity management purposes) which legitimate basis is the consent of both the individual minor and his/her parents

iii) the enrolment of customers (also for identity management purposes in view of the fight against fraud) and the enrolment of volunteers (for experience and research purposes) which legitimate basis is the data subject's consent.

The CNIL is actually much stricter regarding the enrolment of minors and customers than employees for example. The context of implementation of biometric systems (school, work *et cet*…) appears in practice the primary criterion when assessing the proportionality of a system. Technological developments led the CNIL to reconsider its policy, in particular with respect to two of these criteria.

First, the distinction between biometric data leaving trace and biometric data leaving no trace is less and less relevant. This was already noticed by several authors, since rapid technological evolutions show that biometric data that was not considered as "leaving trace" and thus susceptible to be captured and used without the knowledge of the individuals must now be considered as biometric data leaving trace. A striking example is "face recognition", which multiple uses online makes face more and more subject to biometric identification. Another example is finger/hand vein recognition or iris recognition which technological evolution goes towards more and more contactless biometric systems, thus paving the way to possible use without the knowledge of the individual. As noticed by E. Kindt, "*whether biometric characteristics can be captured with or without the presence and/or cooperation or knowledge of the data subject is not neutral as it depends on the state of the art of particular biometric technology at a given moment*"[20], implying that more biometric characteristics may leave traces over the year and become apt for hidden collection and comparison. Aware of these evolutions, the CNIL have abandoned this distinction since mid-2013. Along with other, we believe this new approach is most welcomed.

Second, concerned by the increasing recourse to biometric technologies to identify/authenticate individuals, the CNIL decided to launch in 2012 a deep reflection regarding the use of biometrics in individual's everyday life. The goal of the CNIL was to proactively address the multiplication of biometric identification in everyday life, from the work place to the use of biometric bank credit card or the identification of patients in hospitals, public services, commercial services et cet… This led the CNIL to order a survey regarding the perception of biometrics by the French population. The results showed that the French population widely admits the use of biometric identification by State authorities for national-security and/or forensic purposes.[21] While the use of biometric identification in the work environment receives mixed reactions, the French population is however clearly reluctant to the use of biometric technologies in the commercial context, including biometric contactless payment means or access control to catering or recreational spaces. As a whole, the French population showed to be reluctant to trivial uses of biometrics in the everyday life.

This study shall contribute to reorient CNIL's policy and to emphasize the categories of purposes pursued by the biometric system. Indeed, the CNIL is considering to distinguish three types of systems:

[20] Els Kindt, *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013, p. 655

[21] Sandra HOIBIAN, « Les Français se montrent réservés sur l'usage de la biométrie dans la vie quotidienne », Report of the CREDOC (Centre de Recherches pour l'Etude et l'Observation des Conditions de Vie), May 2013, available here : http://www.credoc.fr/publications/abstract.php?ref=R291

1) "security-related biometric systems", which are those deemed indispensable. In those cases, the biometric system is exclusive and individuals cannot opt-out.
2) "Biometric systems as a service" (also called "biométrie de confort"). In these cases, the security claims are not sufficient to override individual's rights. As a consequence, individuals will have to be duly informed and explicitly consent to be enrolled.
3) "Biometric systems for research or experimental purposes".

1.3 Introduction to the evaluation criteria

Following the extensive research carried out regarding Biometric applications in concrete cases in France and the proportionality policy of the French Data Protection Authority (CNIL)[22], combined with other findings concerning the deployment of biometrics in other EU Member States[23] and input from the Working Party 29[24] and literature[25], essential criteria to assess the proportionality of a biometric system have been identified and extracted in order to provide the basis for an automatic scoring. These criteria are the following:

1) the categories of people to be enrolled in the system
2) The robustness of the legitimacy of the system
3) The functionality of the system & the type of storage of the biometric characteristics

Along with the CNIL's renewed approach, the type of biometric data collected (following the distinction between biometric characteristic leaving trace or biometric characteristic leaving no trace) has however been put aside. This distinction is indeed critical given the technological advances in the field of biometrics, where finger vein or palm vein recognition tends to be collected without the active participation of the individual and may become apt for hidden collection and comparison very soon. In this perspective, this criterion has not been retained in the questionnaire.

1.3.1 **The categories of individuals involved/contexts of deployments of biometric systems**

The risk associated to different categories of individuals has been attributed on the basis of an evaluation of the field, in particular an exhaustive analysis of the situation in France, and an overview of the situation in other EU Member States. It appeared to us that we can, at least, distinguish four main contexts of implementation of biometric systems: 1) Biometric in school environments, 2) Biometrics in professional environments, 3) Biometrics in services environment, 4) Other uses.

Each of these contexts present different impacts on individual's rights to privacy and data protection. In order to assess such impact, we believe that two main aspects can be taken into account. First, we will see why the condition of the data subject combined with the level of maturity of uses of biometrics in a given environment constitutes, according to us, a useful criterion for an impact assessment. Second, we will see how this first basic categories of people

[22] Claire Gayrel, "The principle of proportionality applied to biometrics in France, ten years of CNIL's deliberations", *to be published*

[23] Paul de Hert & Koen Christianen, *Council of Europe Progress Report on the application of the principles of convention 108 to the collection and processing of biometric data*, January 2014.

[24] Article 29 Data Protection Working Party, *Opinion 03/2012 on developments in biometric technologies*, 27 April 2012, WP193

[25] Els Kindt, *op.cit.*, in particular pp. 822-829 and chapter 9 "A legal model for the use of biometric data in the private sector", pp. 831-896.

may be extended in the future and require a concerted evaluation by European Data Protection Authorities.

1.1.1.3 Measuring impact according to the condition of the data subject and the level of maturity of uses of biometrics

It is a particularly difficult and somewhat controversial task to determine the level of impact on privacy according to the condition of the data subject and the level of maturity of uses of biometrics in a given context. For instance, with regard to the condition of the data subject, one may argue that individuals benefit, as a principle, from an equal protection of their fundamental rights under the ECHR and the Charter of Fundamental Rights. In practice, the condition of the applicants before the European Court of Human Rights informs about the circumstances of the case and proved to be an important element in courts judgments, in particular for the interference assessment. With regard to the level of maturity of biometrics uses in a given context, one may argue that this is not because biometrics would be widely used in a professional context that the impact on employees' rights to privacy and data protection may be less important than on customers. Indeed, the debate is open and there may well be different evaluations in different Member States. However, our intention is to provide pragmatic criteria. To do so, we believe that the analysis of the field (see *supra* a summary of the analysis of the situation in France), and by thus of the demand of biometrics (contexts of expansion of biometrics, context of experimentation), should be taken into account.

Therefore, we believe that differentiating the categories of individuals enrolled in a biometric system is a relevant approach in order to apprehend the context where a biometric system is going to be deployed. For each of the four main contexts described above, we therefore distinguish four categories of data subjects and suggest an impact score that could be taken into account for measuring the impact of a biometric system on individual's rights:

Work environment	Employees/habilitated persons	+
Commercial environment	Customers	++
School environment	Minors/pupils	+++
Other	Other	+

Table 7: Table of impacts according to the categories of people enrolled in a biometric system

The above table is based on three main assumptions:

- *Assumption 1: the Enrolment of minors in biometric systems present a higher impact on privacy and data protection than the enrolment of adults considering their age and the fact that their biometric characteristic are non-definitive*.
- *Assumption 2: Among adults, the Enrolment of customers present a higher impact on privacy and data protection than the enrolment of employees since the deployment of biometrics in the commercial environment is likely to make collection of biometric data commonplace and make people less and less aware of the risks associated to the processing of their biometric characteristics.*
- *Assumption 3: the enrolment of volunteers, provided that they express a valid consent, should not be considered as problematic given the interest in encouraging research and innovations.*

These three assumptions can be derived from CNIL's policy over the last decade in the field of biometrics.

1.1.1.4 Further developments?

Of course, there may be other contexts of deployment of biometrics. In our analysis of the situation in France over the last decade, we have crossed several biometric systems that do not enter within the categories of people identified here-above. In one case, we have seen the use of biometrics to identify candidates to an exam organized worldwide and subject to major identity fraud issues. In such case, the condition of the data subject does not enter in neither of these four categories described above. We have also seen some decisions regarding vulnerable people and a decision where the data subjects were enrolled in a biometric system as users of a public service. In our view, being a user of a public service cannot be completely assimilated to a condition of customer and may raise different issues. Besides, we have seen that biometric systems have been experimented in the hospital context for the identification of patients. Finally, although such biometric systems have been installed following the adoption of an executive decree, the deployment of biometrics in prisons and the enrolment of prisoners for monitoring access to visiting rooms may also constitute another specific category of data subjects.

Our contribution does not intend to be exhaustive. Instead, we provide a first pragmatic approach for the evaluation of biometric systems that correspond to major contexts of use of biometrics in the present. Further categories and impact scores should be added and require specific deliberations by European Data Protection Authorities. We will now turn to the criterion of the legitimacy of biometrics.

1.3.2 **The robustness of the legitimate basis**

If in all these contexts, the recourse to biometrics obey to the identity management imperative, we can distinguish two main categories of purposes. Each category of purpose rely on different legitimate basis following article 7 of the directive 95/46. We will explain the necessary conditions applying to each legitimate basis so as to measure the robustness of the legitimacy of the system.

1.1.1.5 Convenience purposes / fight against fraud and conditions for a valid consent

The data subjects' consent constitute the appropriate legitimate basis for the installation of biometric system in the commercial environment and the school environment. It is also applicable to the use of biometrics for research and experimentation purposes, where data subjects shall participate on a voluntary basis.

There is an on-going debate regarding the validity and strength of data subject's consent in the field of data protection. Ensuring the collection of a robust consent has become a primordial issue in view of legitimizing certain data processing. For the record, the data subject's consent is defined in the Directive as "*any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*."[26] For the purposes of our contribution, we have identified a list of requirements that should be respected in order to ensure the collection of a robust consent for the processing of biometric data. The conditions for a valid consent are based on the definition

[26] Article 2 h) of Directive 95/46

above, the Opinions of the Working Party 29 in this respect and on the clarifications that should be brought by the new data protection framework. The conditions applicable to the collection of consent are the following:

- There is no significant imbalance between the position of the data subject and the controller.[27] This condition has been stated by the Working Party 29 in its opinion regarding consent.[28] In the context of employment in particular, the Article 29 Working Party generally considers that there is a strong presumption that the consent is weak in such context considering the subordination relationship between the employer and its employees. This is also the main reason why the consent will not constitute an appropriate legitimate basis for the collection and processing of biometric data in the work environment. Instead, the use of biometric data regarding employees will have to rely on the legitimate interests of the data controller following article 7 f) of the Directive 95/46 (see *infra*).
- The data subject is given the possibility to choose between enrolling in the biometric system or another less privacy intrusive alternative. The individual must have a real choice between enrolling in the biometric system or another means. The recourse to the other means must be free of charge.[29]
- The data subject's refusal to enroll in the biometric system does not entail negative consequences, such as depriving the data subject from benefiting from a service. This is essential in order for consent to be freely given.[30]
- The data subject has the right to withdraw his or her consent at any time. This condition is derived from the Regulation proposal[31] on data protection and the modernization of convention 108.[32]
- The data subject is given all necessary information regarding the processing of his/her biometric data and other personal data prior to his enrollment. This condition is essential in order to ensure the collection of an *informed* consent.

In the case of minors, two further conditions have been identified:

- The age of the minor is not below the age of discernment. It is a difficult decision to establish an age limit for the processing of biometric data. The European Parliament and the Council decided to limit the collection of fingerprint to issue the biometric passport for minors below the age of 12 instead of the age of 6 initially suggested by the European Commission.[33] Moreover, the age of discernment is a general requirement applicable to the capacity to consent under civil law. Finally, such limit allows some difference among Member States.
- Both the minors and his/her parents or legal representative must provide their consent. This condition derives from the practice of DPAs. It is applied by the CNIL[34], but also

[27] This condition is explicitly inserted in the Regulation proposal on data protection in article 7§4

[28] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011, WP187

[29] *Idem*

[30] *Idem*

[31] This condition is explicitly inserted in the Regulation proposal on data protection in article 7§3

[32] See Explanatory Report attached to convention 108 modernized

33 See the procedure 2007/0216(COD) on European passport and travel documents: standards for security features and biometrics

[34] Unique Authorization AU-009 of 27 April 2006, article 6.

recommended by the Irish DPA[35] and British DPA[36], at least. There seem to be a common approach at European level.

1.1.1.6 Security purposes: the different degree of legitimate interests to be balanced with individuals rights

In these cases, the appropriate legal basis is the "legitimate interests" invoked by the data controller. On the basis of our analysis of the uses of biometrics in the work environment in France, we have identified three main categories of legitimate interests invoked by data controllers that translate in our view three levels of legitimacy of the biometric systems.

- Cases of legitimate interests of the data controller only

In this case, the biometric system is set up primarily in view to protect the business or economic interests of the organization/employer. In general, the biometric system aims at controlling access to the work premises in order to prevent theft of goods, property or business secrets. Another important application domain is the use of biometrics to control employee's right to use certain applications/devices

- Legitimate interests of my organization and of other third parties/individuals' interests

In this case, the biometric system is not only set up in view to protect an economic interest of the organization, but also aims at protecting the interests of third parties or individuals. A first example could be the use of biometrics to ensure appropriate protection of the physical integrity of employees (e.g.: an important importer of jewels, subject to potential armed attacks install a biometric to prevent unauthorized access to the factory both in view to protect the employees and the property). Another example could be the use of biometrics to regulate access to classified information or sensitive data. This situation requires a fair balancing between the legitimate interests to be protected and the rights of the employees.

- General public interest

In this case, the biometric system primarily aims at the protection of interests of the wider community, which can qualify as a public interest. A public interest can be qualified when the biometric system aims at controlling access to a critical infrastructure (e.g.: access control to a nuclear power plant) or a laboratory storing dangerous substances/goods.

1.1.1.7 Assessing legitimacy: summary of impact scores

We believe the legitimacy of a biometric system could be evaluated on the basis of the following impact scores. A consent will be deemed valid when all conditions set up above will

[35] See Data Protection Commission of Ireland, Biometrics in schools, colleges and other educational institutions, available here: https://www.dataprotection.ie/docs/Biometrics-in-Schools-Colleges-and-other-Educational-Institutions/409.htm

[36] According to the Information Commissionner « There is nothing explicit in the Act to require schools to seek consent from all parents before implementing a fingerprinting application. However, unless schools can be certain that all children understand the implications of giving their fingerprints, they must fully involve parents in order to ensure that the information is obtained fairly. », see here: http://ec.europa.eu/justice/data-protection/document/national-policy/files/uk_use_biometrics_schools_en.pdf and here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268649/biometrics_advice_revised_12_12_2012.pdf

be satisfied. In contrast, the consent will be deemed weak if at least one of the condition is not respected. With regard to the legitimate interests of the organization, the impact on individuals 'rights will vary according to the nature of the interests to be protected. If such interests essentially relate to those of the data controller, the impact will be deemed higher for data subjects 'rights. In contrast, if the interest at stake are collective and can be qualified "public", the impact on individuals 'rights, the legitimacy of the use of biometrics will increase and the impact on individuals 'rights will be deemed lower.

Work environment	Legitimate interests of the controller only	**+++**
	Legitimate interests of the controller and of third	**++**
	General public interest	**+**
Commercial environment/school environment	Weak consent	**+++**
	Valid consent	**+**
Other	Legitimate interests of the controller only	**+++**
	Legitimate interests of the controller and of third	**++**
	General public interest	**+**
	Weak consent	**+++**
	Valid consent	**+**

Table 8: Table of impact according to the strength of the legitimate basis of the biometric system

1.3.3 **The functionality of biometric systems and type of storage**

This criterion follows from the Working Party 29 opinion, which distinguishes verification systems and identification systems.[37]

A *verification* system is understood here as the process of comparing the biometric data of an individual acquired at the time of the matching with one single biometric template (referred to as a 1:1 matching process). The biometric data may be stored on an individual device[38] or in a central database.[39] The centralized storage is usually considered more intrusive into individual's rights to privacy and data protection than the storage of the biometric characteristic in an individual device. Indeed, the issue of storage in the field of biometrics is crucial for the security of the biometric data. Centralized storage of biometric characteristics, even in the form of templates, presents higher risks in case of accidental loss, alteration, unauthorized disclosure or access.[40]

[37] See the definition and implications of verification systems and identification systems in Opinion 3/2012 of Article 29 Working Party on developments in biometric technologies of 27 April 2012, WP193, pp. 5-6

[38] The biometric data may be stored on a personal device, as a laptop, or on a token or a badge belonging to the data subject.

[39] The centralized storage may be preferred by data controllers when the use of a badge or a token is proved inappropriate in given circumstances (e.g. risks of loss). In this case, the data subject is generally active in order to extract the biometric template from the central database prior to the matching. Most frequently, the extraction/selection of the template in carried out through a PIN code known exclusively by the data subject.

[40] Els Kindt, *op. cit*., pp. 353-363.

In contrast, system of *identification* involves the comparison of a biometric data with a number of previously stored biometric templates (referred to as a 1:n matching process). Such systems necessarily involve the centralized storage of biometric characteristics, although certain security measures may be applied to prevent unauthorized access, but they also present higher risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.[41]

As has also been highlighted by Els Kindt, the functionality of the system (verification v. identification) is crucial for the assessment of the risks to individuals'rights to privacy and data protection. According to Els Kindt, the use of biometric systems for verification systems in the provate sector should be thorougly scrutunized[42], and even prohibited without explicit legal authorization.[43] Besides, she recommends that biometric data shall in principle not be stored in central, distributed or local databases, unless an exemption applies.[44] Indeed, as briefly explained above, centralized storage of biometric data, even for verification purposes, "*poses many risks for the data subjecs, not at least the risk of identification, including the use as unique identifier, but also of re)use and function creep, use of sensitive information, profiling and surveillance, (idendity) theft, and additionally important security risks*."[45]

In the absence of such a specific legal framework for biometrics regulating the use of verification or identification systems and the type of storage, we have to produce evaluation criteria that could be useful in practice for system owners. Our approach is to make them aware of the risks associated to each type of system. We also took into consideration of our analysis of the "field" in France where the decentralized storage of the biometric data (in badges or tokens) proved to be inappropriate in certain situations although biometrics was used for verification purposes and not for identification purposes. In the light of all these elements we decided to allocate the following impact scores based on the criteria of functionality and storage:

Functionality	**Storage**	**Impact score**
Verification +	Storage on an device exclusively under the control of the data subject +	**++**
	Central storage (whether in a central server or in the local reader) ++	**+++**
Identification +++	Central storage of biometric characterictics separated from other identifiers +	**++++**

[41] *Idem*., pp. 647-654

[42] *Idem*, p.649

[43] *Idem.* pp. 839-842

[44] *Idem*, pp. 848-850

[45] *Idem*, p. 848

	Central storage of biometric characteristics and other identifiers altogether +++	**++++++**

Table 9: Table of impacts according to the functionality and type of storage of biometric data

4.5. Impact grid and impact scores

At the end of the first phase, the tool shall automatically generate a preliminary assessment of the proportionnality of the system envisaged. The evaluation is based on the answers provided by the user to 4 main questions/criteria explained in the previous section and summarized hereunder:

Criteria			Risk	Coeff
Categories of persons		Minors	+++	1
		Customers	++	
		Employees	+	
		Other	+	
Legitimacy	Consent	Weak consent	+++	2
		Valid consent	+	
	Legitimate interests	Legitimate interest of the controller only	+++	
		Legitimate interests of the controller and of third	++	
		General public interests	+	
Functionality		Identification	+++	2
		Verification	+	
Storage	Identification	Central storage of biometric characteristics and other identifiers	+++	1
		Central storage of biometric characterictics separated from other identifiers	+	
	Verification	Central storage	++	
		Storage on an individual device exclusively under the control of the individual	+	

Table 10: Table of impacts of biometric systems based on essential proportionality criteria

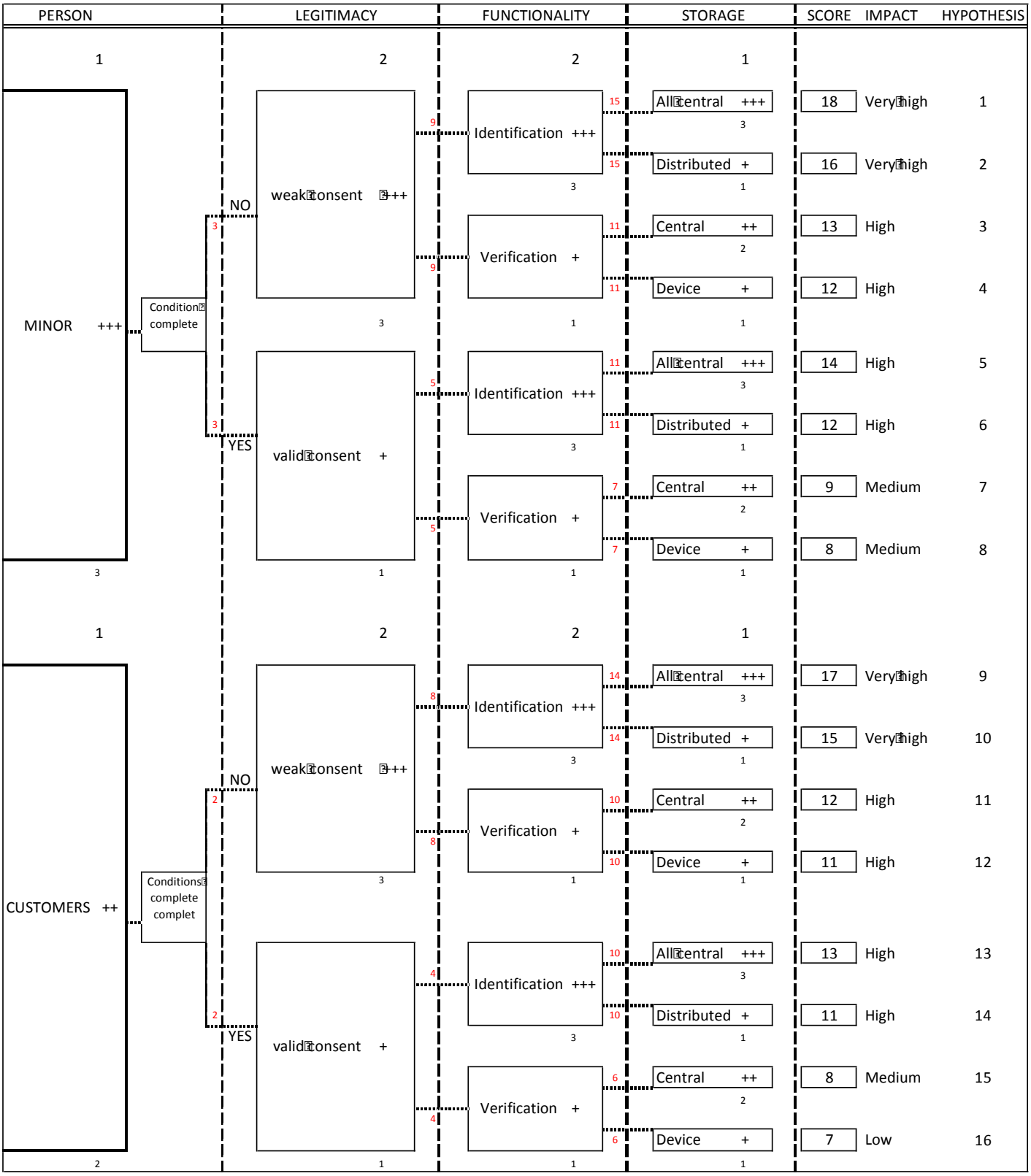
These four criteria leads to 48 different systems, which « impact scores » can be categorized into four levels: ***very high***, ***high***, ***medium*** and ***low*** impact. Hereunder is the scoring grid:

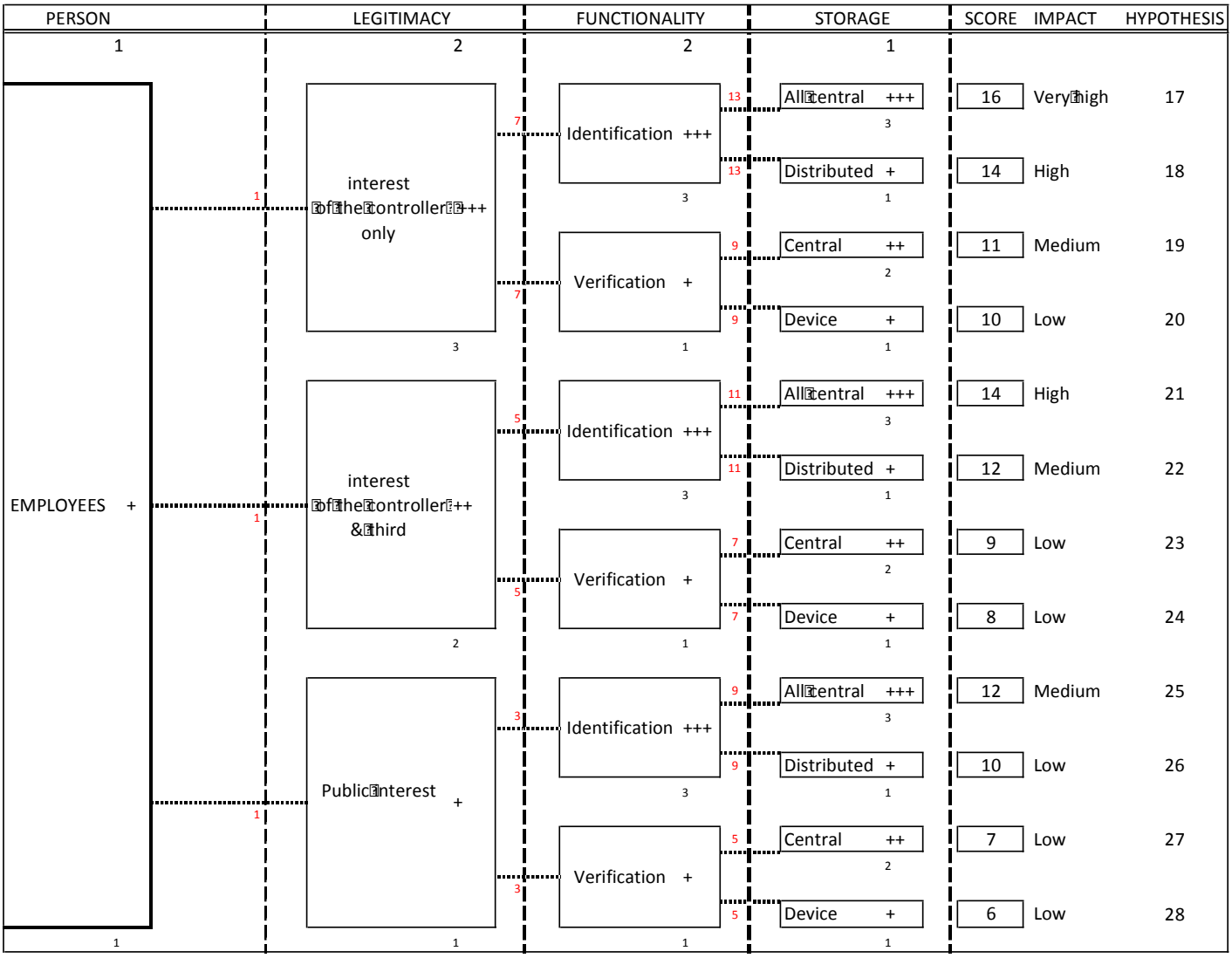
Impact	Consent	Legitimate Interests
Very high	**Score ≥15**	**Score ≥15**
High	**11≤ score < 15**	**13≤ score < 15**
Medium	**8 ≤score<11**	**11 ≤score<13**
Low	**score < 8**	**score < 11**

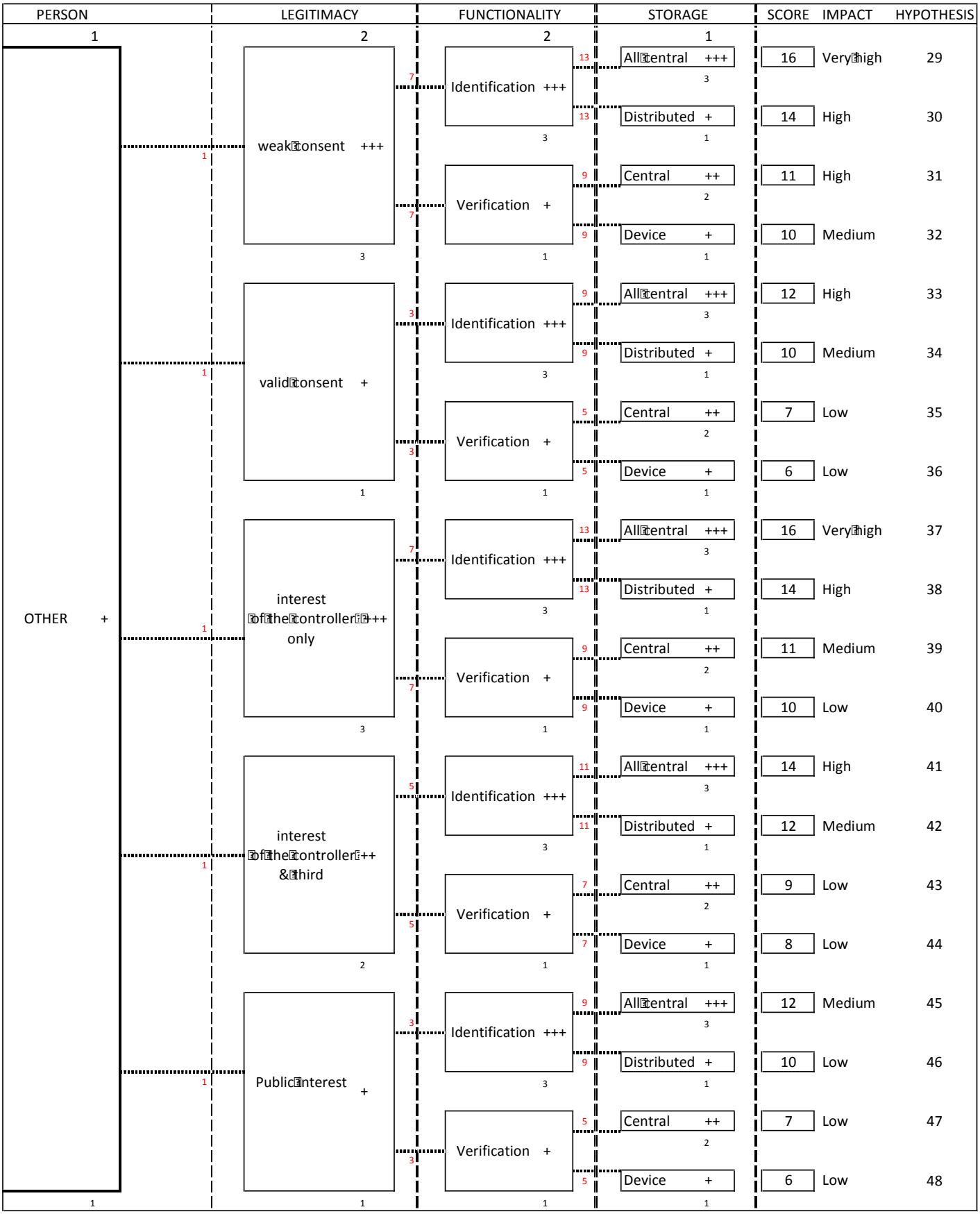
Table 11: Table of impact scores of biometric systems

Systems deemed to involve a "***very high"*** and "***high***" impact are further described as "*likely to involve a disproportionate interference into individual's rights*", while systems deemed to involve a "***medium***" or "***low***" impact will be described as "*likely to involve a disporportionate intereference".*

Following their scores and characteristics, these 48 hypothesis generates 14 different evaluations (several evaluations generating identical scores or comparable impacts for identifcal reasons thay have been categorized altogether to limit the number of evaluations):


PERSON
LEGITIMACY
FUNCTIONALITY
STORAGE
SCORE
IMPACT
HYPOTHESIS
MINOR +++
CUSTOMERS ++
Condition complete
Conditions complete complet
NO
YES
weak consent +++
valid consent +
Identification +++
Verification +
All central +++
Distributed +
Central ++
Device +
18 Very high 1
16 Very high 2
13 High 3
12 High 4
14 High 5
12 High 6
9 Medium 7
8 Medium 8
17 Very high 9
15 Very high 10
12 High 11
11 High 12
13 High 13
11 High 14
8 Medium 15
7 Low 16


PERSON
LEGITIMACY
FUNCTIONALITY
STORAGE
SCORE
IMPACT
HYPOTHESIS
1
2
2
1
EMPLOYEES +
interest of the controller ++ only
interest of the controller ++ & third
Public interest +
Identification +++
Verification +
All central +++
Distributed +
Central ++
Device +
16 Very high 17
14 High 18
11 Medium 19
10 Low 20
14 High 21
12 Medium 22
9 Low 23
8 Low 24
12 Medium 25
10 Low 26
7 Low 27
6 Low 28


PERSON
LEGITIMACY
FUNCTIONALITY
STORAGE
SCORE
IMPACT
HYPOTHESIS
OTHER +
weak consent +++
valid consent +
interest of the controller ++ only
interest of the controller ++ & third
Public interest +
Identification +++
Verification +
All central +++
Distributed +
Central ++
Device +
16 Very high 29
14 High 30
11 High 31
10 Medium 32
12 High 33
10 Medium 34
7 Low 35
6 Low 36
16 Very high 37
14 High 38
11 Medium 39
10 Low 40
14 High 41
12 Medium 42
9 Low 43
8 Low 44
12 Medium 45
10 Low 46
7 Low 47
6 Low 48

- Very high impact: H1, H9, H29

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **very high impact** on individul's rights to privacy and data protection, which is **very likely to involve a disproportionate interference into individual's rights.**

First, the system relies on a weak legitimate basis (not all conditions are satisfied.)

Second, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Third, the system relies on the central storage of biometric information and other identifiers altogether increasing the above-mentioned risks in case of accidental loss, alteration, unauthorized disclosure or access.

Recommandation

You should reconsider the opportunity to deploy the biometric system.

- High to very high impact: H2, H10, H30

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **high to very impact** on individul's rights to privacy and data protection, which is **likely to involve a disproportionate interference into individual's rights.**

First, the system relies on a weak legitimate basis (not all conditions are satisfied.)

Second, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Recommandation

You should consider strictly the necessity to rely on an identification system instead of a verification system.

You should reconsider and fulfill all suggested conditions to ensure the collection of a valid consent.

- High impact: H3, H11, H31

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **high impact** on individul's rights to privacy and data protection, which is **likely to involve a disproportionate interference into individual's rights.**

First, the system relies on a weak legitimate basis (not all conditions are satisfied.)

Second, the system relies on the central storage of the biometric information, which involves more risks in case of accidental loss, alteration, unauthorized disclosure or access.

Recommandation

You should reconsider and fulfill all suggested conditions to ensure the collection of a valid consent.

You should consider stricly the necessity of a centralized storage of the biometric information instead of a decentralized storage on an individual device exclusively held by the individual.

- High impact: H4, H12

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **high impact** on individul's rights to privacy and data protection, which is **likely to involve a disproportionate interference into individual's rights.**

Indeed, the system relies on a weak legitimate basis (not all conditions are satisfied.)

Recommandation

You should reconsider and fulfill all suggested conditions to ensure the collection of a valid consent.

- Medium impact: H32

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **medium impact** on individul's rights to privacy and data protection, which is **likely to involve a proportionate interference into individual's rights.**

However, the system relies on a weak legitimate basis (not all conditions are satisfied.)

Recommandation

You should reconsider and fulfill all suggested conditions to ensure the collection of a valid consent.

- High impact: H5, H13, H33

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **high impact** on individul's rights to privacy and data protection, which is **likely to involve a disproportionate interference into individual's rights.**

First, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Second, the system relies on the central storage of biometric information and other identifiers altogether increasing the above-mentioned risks in case of accidental loss, alteration, unauthorized disclosure or access.

Recommandation

You should consider strictly the necessity to rely on an identification system instead of a verification system.

If the identification system is deemed necessary, you should then consider stricly the necessity of a centralized storage of the biometric information and other identifiers altogether.

- High impact: H6, H14

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **high impact** on individul's rights to privacy and data protection, which is **likely to involve a disproportionate interference into individual's rights.**

Indeed, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Recommandation

You should consider strictly the necessity to rely on an identification system instead of a verification system.

- Medium impact: H34

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **medium impact** on individul's rights to privacy and data protection, which is **likely to involve a proportionate interference into individual's rights.**

However, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Recommandation

You should consider strictly the necessity to rely on an identification system instead of a verification system.

- Low to medium impact: H7, H15, H19, H23, H27, H35, H39, H43, H47

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **low to medium impact** on individul's rights to privacy and data protection, which is **likely to involve a proportionate interference into individual's rights.**

However, the system relies on the central storage of biometric information, which involves more risks in case of accidental loss, alteration, unauthorized disclosure or access.

Recommandation

You should consider stricly the necessity of a centralized storage of the biometric information instead of a decentralized storage on an individual device exclusively held by the individual.

- Low to medium impact: H8, H16, H20, H24, H28, H36, H40, H44, H48

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **low to medium impact** on individul's rights to privacy and data protection, which is **likely to involve a proportionate interference into individual's rights.**

Recommandation

None.

- Very high impact: H17, H37

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **very high impact** on individul's rights to privacy and data protection, which is **very likely to involve a disproportionate interference into individual's rights.**

First, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Second, the system relies on the central storage of biometric information and other identifiers altogether increasing the above-mentioned risks in case of accidental loss, alteration, unauthorized disclosure or access.

As a consequence, the legitimate interests invoked (legitmate interests of your organization only) appear overriden by the interests for fundamental rights and freedoms of the individuals.

Recommandation

You should reconsider the opportunity to deploy the biometric system.

- High impact: H18, H38

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **high impact** on individul's rights to privacy and data protection, which is **likely to involve a disproportionate interference into individual's rights.**

Indeed, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

As a consequence, the legitimate interests invoked (legitmate interests of your organization only) appear overriden by the interests for fundamental rights and freedoms of the individuals.

Recommandation

You should consider strictly the necessity to rely on an identification system instead of a verification system.

- High impact: H21, H41

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **high impact** on individul's rights to privacy and data protection, which is **likely to involve a disproportionate interference into individual's rights.**

First, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Second, the system relies on the central storage of biometric information and other identifiers altogether increasing the above-mentioned risks in case of accidental loss, alteration, unauthorized disclosure or access.

As a consequence, the legitimate interests invoked (legitmate interests of your organization and of third) appear overriden by the interests for fundamental rights and freedoms of the individuals.

Recommandation

You should consider strictly the necessity to rely on an identification system instead of a verification system.

If the identification system is deemed necessary, you should then consider stricly the necessity of a centralized storage of the biometric information and other identifiers altogether.

- Medium impact: H22, H42

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **medium impact** on individul's rights to privacy and data protection, which is **likely to involve a proportionate interference into individual's rights.**

However, the system relies on a function of identification, which involves the central storage of biometric information and presents more risks of further use for incompatible purposes (function creep), tracing or surveillance and identity theft.

Recommandation

You should consider strictly the necessity to rely on an identification system instead of a verification system.

- Medium impact: H25, H26, H45, H46

The evaluation follows from the answers that you provided in the questionnaire. It consists of a preliminary assessment of the potential impact of your biometric system on individul's rights to privacy and its overall legitimacy and proportionality on the basis of four main elements : categories of persons enrolled in the system, robustness of the legitimacy of the envisaged system, functionality of the biometric system and type of storage of the biometric information.

Impact

On the basis of your answers to the questionnaire, the biometric system envisaged presents a **low to medium impact** on individul's rights to privacy and data protection, which is **likely to involve a proportionate interference into individual's rights.**

Indeed, the nature of the legitimate interests invoked (general public interests) may justify the deployment of a biometric system relying on a function of identification. However, such characteristics involve higher risks for the data protection risghts of individuals.

Recommandation

The characteristics of the biometric system requires the adoption of a very high standard of security and the implementation of appropriate organisational measures.

1.4 Conclusions

The criteria retained, namely “categories of persons enrolled”, “legitimacy”, “system functionality” and “type of storage” are not the only criteria that are useful for evaluating the proportionality of a biometric system. As explained in the introduction of the present section, they only constitute essential useful criteria that could/should be supplemented by other criteria. In particular, the evaluation of the necessity or added value of biometrics in comparison with The non-retention of the raw data, biometric template protection measures, the establishment of appropriate fallback procedure in case of false rejection or alternative procedures for people that are unable to enrol constitute further important criteria that should be taken into account in the proportionality analysis. Our goal was certainly not to be exhaustive and provide a tool that would ensure compliance with all data protection obligations. Instead, and as has been underlined in all deliverables, we tried to identify essential criteria in order to assist decision-makers.

The evaluation criteria and score grid suggested to assess the overall proportionality of a biometric system have been submitted for discussion to several stakeholders from a wide range of background. It has been presented to academics, the French data protection Authority (CNIL), the biometric industry (notably Morpho and the European Association for biometrics) and to potential external end-users.[46] Our research and presentations of the criteria and questionnaire was generally well received and perceived as contributing positively to the sensitive issue of the balance between privacy and surveillance in the field of biometrics. We hope that our suggestion of criteria can provide a useful basis for further discussion among relevant stakeholders, including public authorities, in particular in view of the harmonization of approaches between Member States.

[46] See all the details in the Deliverable D8.2 « Plan for use and dissemination »

Annex 2: Assessing the opportunity of a biometric system: questionnaire phase 1

Objectives

This first phase allows you to assess the opportunity to deploy a biometric system, providing you with the steps to carry out a preliminary assessment of the proportionality of the envisaged biometric system with regard to the objectives pursued.

The questionnaire is divided into three categories of questions: purpose, proportionality and legitimacy. Some questions are opened and can be answered freely. Some other are closed questions and will be taken into account in order to generate an automatic preliminary assessment of your system.

1.5 Purposes

1. What is/are the purposes of the biometric system?

Goal: to ensure that biometric data are collected and processed for explicit and specific purpose(s).

Explanation: An explicit, specific, and legitimate purpose for any processing of biometric data is a legal requirement under the data protection directive. The purpose or purposes for which biometric data will be used for must be assessed carefully. You must carry out "an internal assessment". This is the key first step to ensure compliance with applicable data protection law. It is also a necessary condition for accountability. The determination of the purpose or purposes of the biometric system entails legal consequences since as the person or organization defining such purposes you are considered as a "controller" according to data protection legislations and will therefore be the first responsible for compliance with such legislations. As a controller, you must adopt the most thoughtful and reflexive approach on the purposes of the biometric system envisaged.

Expected outcome: The purposes of the processing must be clearly revealed, explained or expressed in some intelligible form, so as to be understood in the same way not only by you (as a controller) and all relevant staff, but also by third-party processors, data protection authorities and the individuals data subjects.

Best practices: Vague or general description of a purpose, such as "security" are not satisfactory. You must be as precise and clear as possible such as: "the purpose of the biometric system is to control employees' access to a local containing dangerous substances".

It is very likely that your first answer will require further improvement when you'll be aware of other questions.

Explain

1.6 Proportionality

2. Is a biometric system *essential* to achieve the purposes pursued?

Goal: To ensure that the biometric system envisaged satisfy the condition of necessity

Explanation: The biometric system should be essential for satisfying the need/purpose rather than being the most convenient and cost effective.

Expected outcome: Here, you should explain the difficulties you are encountering in the management of identity control and which are at the origin of your biometric project.

Explain

3. Have other means, in particular non technological means, been considered? Which are they? And why have these means been put aside?

Goal: to ensure that the recourse to a biometric system is the less intrusive system to achieve the objective pursued.

Explanation: The biometric system should only be chosen after having examined other possible solutions, in particular non-technological solutions.

Expected outcome: Here, it is important that you explain why other possible non-technological solutions have not been retained, or are supplemented by biometric technologies.

Explain

4. On which type of system do you intend to rely? What is the functionality of the system?

Explanation: There are two main categories of biometric systems that rely on two distinct functionalities. These are well known as the functionality of verification (1:1 matching) and the functionality of identification (1:n matching).

☐ **Verification (1:1)**

The verification of an individual by a biometric system is understood in the present questionnaire as the process of comparing the biometric characteristic of an individual (acquired at the time of the verification) to a single biometric characteristic (acquired previously and already stored, whether centrally or on a token). This process is known as a one-to-one matching process (1:1 matching).

☐ **Identification (1:n)**

In contrast with verification, the identification of an individual by a biometric system is understood here in the present questionnaire as the process of comparing the biometric data of an individual (acquired at the time of the identification) to a number of biometric templates (acquired and stored previously, whether on a terminal/reader or in a central database). This process is known as a one-to-many matching process (1:n matching).

5. Where do you intend to store the biometric data?

If "verification"

Explanation: The storage conditions of the biometric data is a crucial aspect of any biometric system. The Working Party 29 strongly advises that whenever it is permitted to process biometric data, it is preferred to avoid the centralized storage of the personal biometric information.

The Working Party considers advisable that biometric systems are based on the reading of biometric data stored on media or any kind of device that are held exclusively by the relevant individuals (e.g. smart cards or similar devices). Their biometric features can be compared with the biometric data stored on the card and/or device by means of standard comparison procedures that are implemented directly on the card and/or device in question, whereby the creation of a database including biometric information should be, in general and if possible, avoided.

Indeed, if the card and/or device is lost or mislaid, there are currently limited risks that the biometric information they contain may be misused. To reduce the risk of identity theft, limited identification data related to the individual should be stored in such devices. Furthermore such decentralized systems provide for a better protection of the biometric data by design as the individual stays in physical control of his biometric data and there is no single point that can be targeted or exploited.

However, for specific purposes and in presence of specific circumstances where the decentralized storage may not be appropriate, centralized storage containing biometric information can be justified. In the context of systems of verification, additional features are nevertheless required to isolate the biometric data in the database in order to process to the verification.

☐ **The biometric data are stored on a device exclusively held by the individual**

Explain briefly the type of device (e.g., badge, laptop, USB key, other…) and why it is personal to the individual.

☐ **The biometric data are stored in (a) central database(s)**

Explain how the biometric data of the individual is isolated in a database for the purposes of the verification process

If "identification"

Explanation: For the identification function, the biometric information has to be stored in a central database. As a result, the biometric data are generally no longer under the control of the individuals. In that perspective, the central storage of the biometric information along with other personal data or not of the individuals raises higher risks of identity theft and potential further use for incompatible purposes (function creep). The central storage is only admissible in a limited number of circumstances, where the function of identification will prove to be necessary and no less intrusive means are available. The central storage covers a wide range of technical implementations from the storage within the reader/terminal to a network hosted database. However, the central storage of the biometric data separated from other identifiers constitutes a reasonable security measure that can contribute to mitigate the risks of identity theft. This is why for the purposes of the evaluation of the opportunity of the biometric system, it is at this stage relevant to distinguish between these two types of storage.

☐ **The biometric data and other identifiers are stored altogether in (a) central database(s)**

☐ **The biometric data is stored in (a) central database(s) without other identifiers**

6. Why do you believe that the biometric system envisaged is the less intrusive mean to achieve the purpose(s) compared to other technological solution?

Goal: to ensure that the recourse to a biometric system is the less intrusive system to achieve the objective pursued.

Explanation: A biometric system should not curtail the right to privacy any more than is necessary to achieve the stated goals. The biometric system should therefore be less intrusive than any other technological solution.

Expected outcome: Here, it is important that you explain why other more "classical" technological solutions have not been retained, or are supplemented by biometric technologies.

Explain

7. Is there evidence that the biometric system have produced, in similar other cases or circumstances, the expected effects?

Objective: to ensure that the biometric system envisaged satisfy the condition of effectiveness.

Explanation: The condition of effectiveness is important to assess the necessity of a system.

Expected outcome: Here, you should provide evidence (if any) or any relevant indication that the envisaged biometric system will effectively meet the objectives pursued.

Explain

1.7 Legitimacy

Under this section, the questions are dynamic.

8. Which categories of data subjects are going to be enrolled in the biometric system?

Goal: to help evaluating the robustness of the legitimacy of the envisaged biometric system in relation to the categories of individuals.

*Explanation: The European Data Protection **Directive 95/46** requires that biometric data (and other kind of personal data) may be collected and processed only under a limited and exhaustive list of circumstances that delineate the legitimate grounds for the processing of personal data. Within the scope of the present questionnaire, there are actually two main relevant legitimate basis. This means that the biometric system envisaged to be set forth must necessarily rely on one of the following grounds in order to be valid:*

- *Consent of the data subject*
- *Legitimate interests pursued by the controller*

The identification of the appropriate legitimate basis for a biometric system is in general closely linked to the categories of data subjects to be enrolled in the system. This is why the questionnaire will automatically select the appropriate legitimate basis according to the category of individuals enrolled.

☐ **Minors**

This category applies notably for the deployment of a biometric system in school environments, or other places frequented by minors.

☐ **Employees**

This category applies for the deployment of biometric systems in the professional environment (access to information systems or use of devices), and in general at work places (access control to work premises).

☐ **Customers/users**

This category applies for the deployment of biometric systems mainly in commercial contexts or public services contexts, when the biometric system aims at controlling the identity of a customer or a user in order to give access to the services.

☐ **Other**

This category applies for all other categories of persons and contexts (e.g. identity control of patients for giving access to certain medical treatment, identity control of volunteers enrolled in an experimentation et cet…)

Detail

If "minors"

Do you satisfy the conditions for the collection of a valid consent?

Explanation: The processing of biometric data of minors is subject to a strict assessment of the legitimacy of the system and therefore requires to pay attention to several factors. Biometric systems within the scope of the present questionnaire, are subject to the consent's of the minors and his parents. According to the European standard definition, the consent of the individual must be specific, clear and freely given in order to be valid.

Expected outcome: You are invited hereunder to check the 5 following conditions in order to assess the robustness of the legitimacy of the intended biometric system. If you cannot satisfy each of the criteria set forth, it means that the envisaged biometric system is likely to lack sufficient legitimacy.

☐ **Minors are old enough to be consulted (age of discernment)**

Explanation: In general, given the specific character of biometric processing, the collection and processing of biometric data of minors should not be envisaged below the age of discernment. Each Member State may have a different position regarding this age limit and you should pro-actively verify at what age it is fixed in the country where the system shall be implemented. You should also check whether the Data Protection Authority has issued any specific recommendation in this respect.

Detail.

☐ **The minor data subject and his/her parents are given the possibility to choose between enrolling in the biometric system or another less privacy intrusive alternative.**

Explanation: As in this case, data subjects are minors, data subject's consent should be complemented by parents 'consent. According to the European standard, the consent of the individual must be specific, clear and freely given in order to be valid. In that aim, the minors data subjects and his/her parents must have a real choice between enrolling in the biometric system or another means.

Explain the alternative

☐ **The minors' refusal <u>or</u> parents 'refusal to enroll in the biometric system does not entail negative consequences, such as depriving the minor from benefiting from a service.**

<u>Explanation:</u> The sole choice between not using a service and giving one's biometric data is a strong indicator that the consent was not freely given and cannot be considered as a legitimate ground.

<u>Best practices:</u> the fact to refuse to enroll in the biometric system and to opt for the alternative system in place must not involve additional costs. For that, the option to enroll in the biometric system must not be at lower price than the alternative system, otherwise it constitutes an incentive that deprive the individual from a real choice;

☐ **The minor <u>or</u> his/her parents have the right to withdraw his or her consent at any time.**

<u>Explanation:</u> This is a logical counterpart of a "freely given" consent. If the data subject is given a real choice, he should then be able to further withdraw his consent. The same possibility should be granted to parents.

☐ **The minor <u>and</u> his/her parents will be given all necessary information regarding the processing of his/her biometric data and other personal data prior to his enrollment**

<u>Explanation:</u> again, in order to be "informed", the individuals data subjects will have to be properly informed.

If "Employees"

Which legitimate interests do you invoke as justifying the processing of biometric data of employees?

<u>Explanation:</u> Most generally, because of the imbalance between the employees and their employer, employee's consent is not considered to provide a valid legal ground for the processing of biometric data in the employment context. The processing of biometric data of employees will therefore find its justification in 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.

There is a variety of legitimate interests for which an organization may be interested in processing the biometric data of its employees. The controller can rely on such legal ground only when he provides the demonstration that his interests objectively prevail over the rights of the

data subjects not to be enrolled in the system. While it is not possible to address all situations, it is nevertheless useful to distinguish between three situations.

☐ **Legitimate interests of my organization only**

Explanation: In this case, the biometric system is set up primarily in view to protect the business or economic interests of your organization.

Ex 1. the biometric system aims at controlling access to the work premises in order to prevent theft of goods, property or business secrets.

Ex. 2. The biometric system aims at controlling employee's right to use certain applications/devices

Detail

☐ **Legitimate interests of my organization and of other third parties/individuals' interests**

Explanation: In this case, the biometric system is not only set up in view to protect an economic interest of your organization, but also aims at protecting the interests of third parties or individuals.

EX. 1. The biometric system aims at ensuring appropriate protection of your employees
As an important importer of jewels, your factory is vulnerable to armed attacks. The biometric system will aim at preventing unauthorized access to the factory both in view to protect your employees and your property.

Ex. 2. the protection of classified information or sensitive data

This situation requires a fair balancing between the legitimate interests to be protected and the rights of your employees.

Detail

☐ **General public interest**

Explanation: In this case, the biometric system primarily aims at the protection of interests of the wider community, which can qualify as a public interest.

Ex. 1. The protection of critical infrastructure

Ex. 2. The protection of dangerous substances/goods

Detail

If “customers”

Do you satisfy the conditions for the collection of a valid consent?

Explanation: The processing of biometric data of individuals in the commercial context must rely on the customer’s consent. According to the European standard definition, the consent of the individual must be specific, clear and freely given in order to be valid.

Expected outcome: Hereunder are identified the minimum conditions for consent to be a valid legitimate ground. The organization shall check each of these conditions. If all conditions are considered to be satisfied, this may constitute an indication that the processing of biometric data is validly grounded. Otherwise, you should reconsider the recourse to the envisaged biometric system.

You must check the whole following conditions:

☐ **There is no significant imbalance between the position of the individual and the organization/person responsible of the biometric system.**

Explanation: Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the individual and the organization setting up the biometric system (controller).

In general, in the commercial context, the relationship between data subjects and the service or product provider will not be found to be significantly unbalanced. However, this balanced relationship must be assessed in the light of the other conditions set forth below.

☐ **The individual is given the possibility to choose between enrolling in the biometric system or another less privacy intrusive alternative.**

Explanation: The individual must have a real choice between enrolling in the biometric system or another means. The recourse to the other means must be free of charge.

Best practice: In order to control access to subscribers to an amusement park, the subscribers are given the choice between enrolling in a biometric system or another non biometric means.

Explain the alternative and how you will ensure that the individual is aware of such alternative

☐ **The individual's refusal to enroll in the biometric system does not entail negative consequences, such as depriving the data subject from benefiting from a service.**

Explanation: The sole choice between not using a service and giving one's biometric data is a strong indicator that the consent was not freely given and cannot be considered as legitimate ground.

Best practices: the fact to refuse to enroll in the biometric system and to opt for the alternative system in place must not involve additional costs. For that, the option to enroll in the biometric system must not be at lower price than the alternative system, otherwise it constitutes an incentive that deprive the individual from a real choice

☐ **The data subject has the right to withdraw his or her consent at any time.**

Explanation: This is a logical counterpart of a "freely given" consent. If the data subject is given a real choice, he should then be able to further withdraw his consent.

☐ **The data subject is given all necessary information regarding the processing of his/her biometric data and other personal data prior to his enrollment**

Explanation: again, in order to be "informed", the individuals data subjects will have to be properly informed. The Questionnaire will come back further on this issue.

If "other"

On which legal ground are you relying on as proving a legitimate basis for the implementation of the biometric system?

Explanations: The biometric system envisaged must necessarily rely on one of the following grounds in order to be valid:
- Consent of the individual (article 7 a) of the directive 95/46)
- Legitimate interests pursued by your organization (article 7 f) of the directive95/46)

You must carefully examine the information provided in relation to each of the two situations and assess which one is the most likely to apply in your situation. The sub-questions drafted hereunder will help you to assess whether the envisaged biometric system is likely to be valid or not.

☐ **Consent of the individual**

☐ **Legitimate interests pursued by the organization/person responsible of the biometric system**

If "consent"

Do you satisfy the conditions for the collection of a valid consent?

Explanation: The data subject's consent must be specific, clear and freely given in order to be valid. "Hereunder are identified the minimum conditions for consent to be a valid legitimate ground. The organization shall check each of these conditions. If all conditions are considered to be satisfied, this may constitute an indication that the processing of biometric data is validly grounded.

You must check and ensure compliance with the whole following conditions:

☐ **There is no significant imbalance between the position of the individual and the controller.**

Explanation: Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

☐ **The data subject is given the possibility to choose between enrolling in the biometric system or another less privacy intrusive alternative.**

Explanation: The individual must have a real choice between enrolling in the biometric system or another means. The recourse to the other means must be free of charge.

Explain the alternative

☐ **The data subject's refusal to enroll in the biometric system does not entail negative consequences, such as depriving the data subject from benefiting from a service.**

Explanation: The sole choice between not using a service and giving one's biometric data is a strong indicator that the consent was not freely given and cannot be considered as legitimate ground.

☐ **The data subject has the right to withdraw his or her consent at any time.**

Explanation: This is a logical counterpart of a "freely given" consent. If the data subject is given a real choice, he should then be able to further withdraw his consent.

☐ **The data subject is given all necessary information regarding the processing of his/her biometric data and other personal data prior to his enrollment**

Explanation: again, in order to be "informed", the individuals data subjects will have to be properly informed. The Questionnaire will come back further on this issue

If “legitimate interests”

Which legitimate interests do you invoke as justifying the processing of biometric data?

Explanation: The Directive provides that the processing of personal data can be justified where “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.” The controller can rely on such legal ground only when he provides the demonstration that his interests objectively prevail over the rights of the data subjects not to be enrolled in the system.

There is a variety of legitimate interests for which an organization may be interested in processing the biometric data of individuals. While it is not possible to address all situations, it is nevertheless useful to distinguish between three situations.

☐ **Legitimate interests of my organization only**

Explanation: In this case, the biometric system is set up primarily in view to protect the business or economic interests of your organization.

Ex 1. the biometric system aims at limiting access to invited visitors to specific premises in order to prevent theft of goods, property or business secrets.

Detail

☐ **Legitimate interests of my organization and of other third parties/individuals’ interests**

Explanation: In this case, the biometric system is not only set up in view to protect an economic interest of your organization, but also aims at protecting the interests of third parties or individuals.

Detail

☐ **General public interest**

Explanation: In this case, the biometric system primarily aims at the protection of interests of the wider community, which can qualify as a public interest.

***

At the end of this first stage of the biometric questionnaire, a first report is generated by the system with the impact evaluation and + recommendations to consult stakeholders are issued.

In relation to consultation of stakeholders, the following message shall be displayed:

"*We recommend that you consult relevant the stakeholders affected by the use of the system you intend to design in order to check the level of acceptability of the system and to identify additional privacy concerns*"

The questionnaire shall suggest a link to come back to the general questionnaire on stakeholder consultation and a link for the recommendations for the processing of biometric data of minors or employees, if relevant.

Annex 3. Consultation of stakeholders

Together with the report generated at the end of Phase 1, the user is recommended to organise a first round of consultation of stakeholders. He/she is given access to the general questionnaire on stakeholders' consultation and if he/she has indicated that the processing involves the processing of biometric data relating to ***minors*** or ***employees***, she is given access to the recommendations.

1.1 Consultation of stakeholders: General questionnaire

1.1.1 Objectives of the questionnaire

In order to fully define the context of the personal data processing activity, it is necessary to identify its implications and expected benefits for the entity but also for individuals and organizations impacted by the processing, be it citizens or technology providers. Under Art. 32.4 of the Draft General Data Protection Regulation, the consultation of data subjects or their representatives would become a legal obligation.

This means opening channels of participation but also implementing a process to take these concerns into account and inform stakeholders about the results of the consultation process, explaining why certain concerns were taken into account while other were discarded. This consultation process is time consuming but it is crucial to obtain the views of people or entities not directly involved in the project, thus able to provide a broader perspective. It can serve to highlight risks that were not spotted in the first place.

The consultation process enhances the transparency of the organization and of the project. It allows the organization to make a commitment to respond to and balance the needs of stakeholders in its decision-making processes and activities and delivers against this commitment. It is a process for learning. The ultimate goal of consultations is to generate ownership of decisions and projects and to enhance the sustainability of activities.

If the organization decides to engage towards a proactive approach and becomes accountable to its stakeholders, the organization One World Trust has for instance developed an accountability framework to provide guidance to organizations on how to operationalize accountability. Five dimensions should be taken into account when designing accountability mechanisms: drafting an accountability strategy, transparency, participation, evaluation, and complaint and response mechanisms. More information can be found here.

The goal of this section is less ambitious. It aims to help the user to identify the stakeholders who should be consulted and suggest ways to organize the consultation and to integrate the views to the decision-making process (the PIA). To that end it guides the user through an open questionnaire.

When should this consultation process be carried out? As general recommendation, it is recommended to carry out the consultation process ***once the opportunity to design the system has been assessed and before the mitigation measures are decided upon.*** The consultation process fully participates from the definition of the risks inherent to the data processing activity. A second round of consultation could occur after the options for the design system have been taken in order to check to what extent they meet users' concerns.

Sources:

- One World methodology
- OECD report on stakeholder consultation process
- CNIL PIA manual

- Spanish DPA's PIA manual

1.1.2 Questions

1. Who are the persons or groups that can affect or be affected by the surveillance system you intend to deploy?

Goal of the question: *Make the organization aware of who its stakeholders are for this data processing activity and which types of commitments the organization have towards them.*

Explanation: *Identifying who your stakeholders are is the first step in having a clear view on which commitments and obligations the organization should comply with. It is also the first step in understanding the different expectations these stakeholders might have and the different forms of responsiveness and accountability which can be inferred from these relationships.*

Stakeholders are individuals and groups that can affect or are affected by an organization's policies and/or actions. Stakeholders can be internal to the organization (e.g. employees, shareholders) or external to the organization (individuals or groups who are affected by an organisations' decisions and activities but who are not formally part of the organization – e.g. data subjects, parents of the minors whose data are processed, contractors).

Stakeholders have different capacity (resources, knowledge and expertise), different degrees of access to reliable information and different needs and expectations.

Best practice: *The organization One World Trust has for instance developed an accountability framework to provide guidance to organizations on how to operationalize accountability. Five dimensions should be taken into account when designing accountability mechanisms: drafting an accountability strategy, transparency, participation, evaluation, and complaint and response mechanisms. More information can be found **here**.*

2. How do you think your system will affect your stakeholders?

Goal of the question: *By clarifying the initial ideas the organisations have about the personal data processing activities, it becomes possible to check whether they conform to reality.*

Explanation: *To answer this question you should take into account the impact the data processing activity might have on privacy (of the body, location, communications, etc.) but also on other aspects such as right to move anonymously, freedom of association, etc. Other impacts such as ethical issues (e.g. impact on the life of the workers) and technical issues (e.g. for service providers) should be considered.*

Best practice: n/a.

3. What are the objectives of the consultation process for each of the stakeholders?

Goal of the question: *Clarifying the goals of the consultation allows to focus the content of the consultation and to assess whether the process has been successful.*

Explanation: *It is paramount to define the goals and objectives of the consultation process, i.e. what the organization wants to achieve by setting up such participatory decision-making. They form the benchmark against which progresses and results can be assessed and start a learning process. Examples of objectives are: identify additional concerns, raise awareness about the processing, involve actively stakeholders in the decision-making process to enhance its transparency.*

How much involvement the organization can or wishes to offer must be clearly defined and clearly communicated to potential stakeholders at the outset of the program. Organisations should also be aware that stakeholders may desire, expect or be entitled to a particular level of involvement.

Three classes of effects may result from the application of consultation and deliberation techniques:

- *Substantive effects (concrete decision outcomes) include: better, more acceptable choices from legal, ethical, economic, and technical points of view*
- *Procedural effects (modifications to the process of deciding) include: better integration of the wider context that determines the range of choices for the decision, opening up the domain of choices considered, more dynamic process, better conflict management, increased legitimacy of the decision making process, improvement of the process in terms of costs and time, improvement of the power of influence of less organised interests, improvement of the quality of the informational basis of the decision process and better use of information*
- *Contextual effects ("side" effects) include: better information to stakeholders and/or to the public, improvement of strategic capacity of decision makers, changes in the perception and conceptualization of the social context, modification in traditional power relations and conflicts, reinforcement of democratic practices within the organisation, increased confidence in the organisation.*

4. Which consultation process will you use for each stakeholder?

Goal of the question: *Help the user to define the most adequate channel of participation for the organization.*

Explanation: *At different phases, involvement may take the form of sharing information, consulting, dialoguing, or deliberating on decisions. The techniques that will be suitable for a particular situation will depend on the stakeholders to be engaged , and the aims and objectives of the consultation. It should also take into account the constraints of the organisations and of the targeted stakeholders.*

Planners should be aware that stakeholders may desire, expect or be entitled to a particular level of involvement. In that regard, the OECD guidelines for stakeholders' involvement warn about the following pitfalls:

- *Consulting the public when the legal scope for them to influence the decision is small causes anger, so it is important to be clear on what issues reasonably can be influenced*
- *The basis for the decision must be clearly understood*
- *It is important to be clear about the information sought and the feedback to be provided by the decision maker*
- *People want to see that they have influenced the process and have had a meaningful impact on the outcome.*

***If the goal is to inform or educate**, this implies developing appropriate public information materials. Information materials will be useful only if they can be understood and interpreted by their intended audience. Each should be adapted to the "starting position" of the stakeholder.*

*Gathering information from stakeholders is sometimes accomplished by **large-scale consultation techniques (polls or surveys).** Survey items will deliver meaningful results only if they are built up from an understanding of how people indeed construe the issues explored by the survey.*

***Higher levels of involvement** usually imply that participants will have the opportunity to communicate their views and judgments in detail, as well as learn from other stakeholders.*
Planners of stakeholder involvement in technical areas will probably benefit from advice on communicating about risks, translating complex information into readily accessible form, and interacting with a range of stakeholders who may not have technical training.

*Finally, a planner may wish to make a **broad announcement of stakeholder initiatives,** or publicize their outcomes using the mass media.*

The table below summarizes the different activities that could be taken to involve stakeholders in the definition of risks and the decision-making process

Low level of public involvement or influence		Mid level	High level of public involvement or influence	
Inform, educate, share or disseminate information	Gather information, views	Discuss through two-way dialogue	Fully engage on complex issues	Partner in the implementation of solutions

Table 12: A public involvement continuum.(c) OECD 2004, "Stakeholders involvement techniques", p.17

Guidance on choosing different levels of public involvement © OECD 2004, "Stakeholders involvement techniques", p.19:

Inform/educate when:	• Factual information is needed to describe a policy, programme or process

	• A decision has already been made (no decision is required) • The public needs to know the results of a process • There is no opportunity to influence the final outcome • There is need for acceptance of a proposal before a decision may be made • An emergency or crisis requires inmediate action • Information is necessary to abate concerns or prepare for involvement • The issue is relatively simple
Gather information/views when:	• The purpose is primarily to listen and gather information • Policy decisions are still being shaped and discretion is required • There may not be a firm commitment to do anything with the views collected – in this case, advise participants from the outset
Discuss or involve when:	• Two-way information exchange is needed • Individuals and groups have an interest in the issue and will likely be affected by the outcome • There is an opportunity to influence the final outcome • Organizer wishes to encourage discussion among and with stakeholders • Input may shape policy directions and programme delivery
Engage when:	• It is necessary for stakeholders to talk to each other regarding complex, value-laden decisions • There is a capacity for stakeholders to shape policies that affect them • There is opportunity for shared agenda setting and open time frames for deliberation on issues • Options generated together will be respected
Partner when:	• Institutions want to empower stakeholders to manage the process • Stakeholders have accepted the challenge of developing solutions themselves • Institutions are ready to assume the role of enabler • There is an agreement to implement

	solutions generated by stakeholders

Best practice: *See as a way of example, the guide published by the OECD on Stakeholders' Involvement Techniques (2004).*

5. **Which information should be presented to the stakeholders?**

Goal of the question: *The way how information is presented to stakeholders will condition their ability to provide meaningful feedback. The information provided and its format is thus highly dependent on the objectives set for the consultation.*

Explanation *Take the opportunity to inform stakeholders about the content of the processing, in compliance with the information requirements contained in the application Data Protection Act. In particular, the communicated information should include the purposes for which the biometric data would be processed (e.g., speeding up access to a catering service), the legitimate interests of the data controller to collect biometric data; the (preliminary) proportionality analysis, the period for which the personal data would be stored; the possibility to object to the processing; where applicable, information about the existence of profiling, or measures based on profiling, and the envisaged effects of profiling on the data subject; and meaningful information about the logic involved in any automated processing.*

The consultation process should however also provide information about the privacy risks analysis performed and explain the reasons that motivated the options taken to develop the system. This includes the nature of the risk identified, the reasons why you identified this to be a risk, the interests at stake and the measures taken to reduce this risk.

Best practice: n/a.

1.2 Recommendations

In order to give examples of potential consultation processes in practice, some recommendations are attached to the questionnaire developed in relation to WP6 use case (biometric technology for access control). These recommendations concern two types of data subjects affected by the processing and who are more vulnerable: ***minors*** and ***employees***.

1.2.1 Minors

1.1.1.1 General information concerning the processing of personal data relating to minors

- From the legal point of view, children constitute a specific category of individuals. Children are entitled to the same legal protection of their fundamental rights, including the right to privacy and the right to data protection (e.g., privacy), as adults, yet they have a limited legal autonomy to act (e.g., to provide consent or to conclude a contract). Often, children are subject to age-specific regulation, reflecting national practices and culture. Some illustrative examples of such cases in the EU could be the different minimum age for compulsory education, employment and consent to medical treatment or sexual activities.
- The EU data protection framework, which is set forth by Directive 95/46/EC, does not entail specific provisions on the processing children's data. However, in practice,

national laws implementing the Directive foresee diverse requirements with respect to the processing of children's personal data. For example, in the United Kingdom ("UK") the parental consent is required to legitimise the processing of children's biometric data till the age of 18, while for the other types of personal data the UK national data protections authority ("DPA") recommends the bright-line of 12 years. The Irish DPA holds a position that in the context of biometric systems at schools, child's consent till the age of 18 should be accompanied by parental consent. Other European countries, such as Lithuania, do not specify requirements for the processing of children's biometric data, but provide for a detailed list of information that can be processed in the school context. In Spain data controllers are obliged to obtain parental consent for the processing of children's personal data till the age of 14, while the Belgian DPA considers the age of 12-14 years to be limit from which onwards the parental consent is no longer needed. In Sweden, the national DPA considers the age of 13 to be the bright-line.

- Provided the fragmented implementation of the EU data protection framework, a data controller, prior to launching an information system that would process children's (biometric) data, should consult a national legislative framework outlining obligations for the processing of children's personal data. Such country specific legal obligations could include the age limit for parental consent, requirements for the processing of biometric data, and types of personal data that can be processed at school.
- The current regulatory framework is expected to change, once the proposed General Data Protection Regulation ("GDPR") is adopted. While the outcome of the GDPR is uncertain, the processing of children's personal data or biometric data, with some exceptions, may be prohibited or subject to strict rules. For example, the processing of special categories of data, such as biometric data, may be allowed on a condition that the explicit consent has been obtained. The proposal for GDPR requires data controllers to consult stakeholders' in situations where the processing operations that would entail the processing of biometric or children's data.
- At the moment, consulting stakeholders, including children, is not mandatory by the data protection framework, yet national DPAs (e.g., the UK DPA) regard it as a good practice. Consulting children also aligns with the ideas established in the UN Convention on the Right of Child, in particular, their right to be consulted and to have their views taken into account in a decision-making process that concerns them (Article 12.1 of the UNCRC). Therefore, data controllers are recommended to consult children, their "legal guardians", and other persons who may be affected through the life-cycle of the system, prior to deploying systems processing children's biometric data.

1.1.1.2 Recommendations linked to the consultation process.

When consulting stakeholders about an information system that will process minors' biometric data, data controllers (or processors acting on the behalf of a controller) are recommended to:

1. **Identify the relevant stakeholders of the information system that will process children's biometric data.**
    a. In addition to children and their legal representatives (e.g., parents or legal guardians), there are other people who could be present in the environment of the system and who may be affected by the system. For example, in situations where a biometric system would be used to facilitate the borrowing of library books, librarians could be included in the consultation, whereas in situations,

where a biometric system would be used to speed up the management of payments for a meal at a canteen, canteen workers could be consulted.

b. To ensure that best interests of children are considered, it is recommended to consult a wide range of stakeholders (e.g., children, their legal representatives, teachers, librarians, canteen workers, and the parent council) who may be directly or indirectly affected by the system.

2. **Identify the age of minors you want to consult, when preparing for a consultation.**
    a. Depending on the age of children and national legislation, it may be necessary to include their legal representatives into the consultation process. For example, the Lithuanian DPA recommends to include parents in the school context as far as the processing of children's personal data is concerned, while in other contexts children can agree to the processing of personal data without prior obtaining parental consent.
    b. It is important to identify the age of minors' (i.e., a target group) who will be contacted at the early stage of the consultation process because it can determine the overall approach of the consultation. It can allow to tailor your consultation to the needs and cognitive capacity of minors or other stakeholders.
    c. Research has shown a low quality of one-to one verification of identity of children under the age of 6, therefore, it is recommended not to process biometric data of children younger than this age. The age of 12 or 14 years is considered to be an acceptable age for the processing of biometric data. This age limit is also used for large-scale IT systems on the EU level (e.g., EURODOC and VIS).
3. **Consider the age-appropriate language to explain information related to the processing of personal data.**
    a. The language used in a communication to children should be clear and plain language, adapted to the data subject (Article 11 of the GDPR).
    b. In a situation, where parents and legal guardians are involved in a consultation process, information provided to them should be adapted to their cognitive capacities to understand information about the matter.
    c. The recommendation to use an age-appropriate language is not only echoed in the Draft General Data Protection Regulation (Article 11 of the GDPR) but is also supported by national data protection authorities in the UK, Spain, Portugal, Poland, and Germany.
    d. To ensure the use of age-appropriate language, pilot your questions with a few representatives of the targeted groups.
4. **Consider employing the age-appropriate means of communication to reach the targeted group(s).**
    a. Different means of communication can be employed to consult children, their representatives and others affected by the system. Alternatives to typical print materials (e.g., surveys or broachers) could be workshops, games,

demonstrations of the system, voting and electronic communications via online questionnaires.

b. Consider of providing a training program for the people who will carry out the consultation.

c. Consider the time that is needed to contact children, their legal representatives and others affected by the system.

5. **Consider ways to raise awareness about the risks of the information processing.**
   a. One of the risks of processing children's biometric data in their daily activities (e.g., school environment) is that the public may become desensitised to the excessive use of their personal data. Therefore, a data controller (or processor acting on the behalf of a controller) should explain in an accessible way the risks that are associated with the particular information system to children, their parents or legal guardians and others affected by the system.
6. **Provide all relevant information related to the processing of children's biometric data.**
   a. Information communicated to children, their parents or legal guardians and other stakeholders about the possibility of introducing an information system for the processing of children's biometric data, should include typical information provided in the information notice (Article 14 of the GDPR). In particular, the communicated information should include the purposes for which the biometric data would be processed (e.g., speeding up access to a catering service), the legitimate interests of the data controller to collect biometric data; the (preliminary) proportionality analysis, the period for which the personal data would be stored; the possibility to object to the processing; where applicable, information about the existence of profiling, or measures based on profiling, and the envisaged effects of profiling on the data subject; and meaningful information about the logic involved in any automated processing.
   b. Provide information about the privacy risks analysis performed and explain the reasons that motivated your choices. Such reasons could include information about the nature of the risk identified, why you considered this to be a risk, the interests at stake and the measures taken to reduce this risk.
7. **Choose a method to collect and record information provided by children and other stakeholders on the proposed system.**
   a. Information provided by children and other stakeholders may include comments, ideas, concerns and other input. To ensure accountability of the decision-making process it is important that this information is properly documented and captured.
   b. In case you want to collect personal data from children, you may need to obtain parental consent and approvals from complement authorities (e.g., the city council and the board of education).
   c. Consider techniques to analyse received information.
8. **Question stakeholders about potential risks and alternative solutions to the proposed system.**

a. Stakeholders are typically better acquainted with the environment where system will be deployed. Therefore, they may be in a position to better identify risks and foresee alternative solutions to the proposed system.
b. In case of deploying a biometric system, alternative solutions should be provided in case a child, a parent or a legal custodian objects to the processing of child's biometric data.

9. **Ensure accountable and objective decision-making process.**
    a. The stakeholders' consultation is a part of the Privacy Impact Assessment. Stakeholders' views and opinions depend on their competences, knowledge and experience. While stakeholders views should play an important role in the decision-making process of a biometric system, careful balancing of stakeholders' views, controller' interests and legal requirements (e.g., the proportionality principle) is required.
10. **Communicate the findings of the consultation process to children, parents and legal guardians as well as other involved parties.**
    a. Consultation is a two-way communication. Thus, the findings of the consultation as well as measures taken in response to the collected information should be communicated back to the minors, their legal representatives and other involved parties. When providing feedback on the consultation, a data controller could explain how it has incorporated the received comments into the design of a system.
    b. Consider carrying out a follow up consultation after a certain time the system is running (e.g., one year).
11. **Consider applicable requirements for the ethical screening.**Ethical screening requirements for the processing of children's data vary per country, institution and field. For example, in the UK, schools often have a parent council that is involved in the decision-making process. In some other countries, such as Germany, regional or local competent authorities governing education matters may need to be consulted prior to launching children's biometric information systems at schools.

1.1.1.3 Sources

1. The relevant provisions of the GDPR (as well as their amendments) on an information notice, consent, and PIA.
2. Opinions of Article 29 WP and the EDPS on information notice, consent, the processing of children's and biometric data.
3. National data protection requirements for consent and DPAs opinions on the processing of children's/ biometric data.
4. General guidance on consulting children.
5. Other media (e.g., blog posts, news reports, etc).

Consulted provisions of the GDPR

Institution	GDPR text
Commission's proposal 2012	**Article 4** (11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data. (18) 'child' means any person below the age of 18 years. **Article 8** Processing of personal data of a child 1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian . The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology **Article 11** 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child. Article 17 Right to be forgotten and to erasure 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons. **Article 33.2 (d)** 1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact

	of the envisaged processing operations on the protection of personal data. 2. The following processing operations in particular present specific risks referred to in paragraph 1: (d) personal data in large scale filing systems on children, genetic data or biometric data.
Parliament's amendments 2014	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. ***Where data processing is based on the data subject's consent in relation to the offering of goods or services directly to a child, consent should be given or authorised by the child's parent or legal guardian in cases where the child is below the age of 13. Age-appropriate language should be used where the intended audience is children. Other grounds of lawful processing such as grounds of public interest should remain applicable, such as for processing in the context of preventive or counselling services offered directly to a child.*** 31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation. ***In case of a child or a person lacking legal capacity, relevant Union or Member State law should determine the conditions under which consent is given or authorised by that person.*** **Article 8. Processing of personal data of a child** 1. For the purposes of this Regulation, in relation to the offering of ***goods or*** services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or ***legal guardian*** . The controller shall make reasonable efforts to ***verify such*** consent, taking into consideration available technology ***without causing otherwise unnecessary processing of personal data*** . ***1a. Information provided to children, parents and legal guardians in order to express consent, including about the controller's collection and use of personal data, should be given in a clear language appropriate to the intended audience.*** 2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child. 3.The ***European Data Protection Board*** shall be ***entrusted with the task*** of ***issuing guidelines, recommendations and best practices*** for the methods ***of verifying*** consent referred to in

	paragraph 1***, in accordance with Article 66.*** ***Article 11*** 1. The controller shall have ***concise,*** transparent***, clear*** and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, in particular for any information addressed specifically to a child. ***Article 19: Right to object*** ***1. The data subject shall have the right to object at any time to the processing of personal data which is based on points (d) and (e) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.*** ***2. Where the processing of personal data is based on point (f) of Article 6(1) , the data subject shall have at any time and without any further justification, the right to object free of charge in general or for any particular purpose to the processing of their personal data.*** ***2a. The right referred to in paragraph 2 shall be explicitly offered to the data subject in an intelligible manner and form, using clear and plain language, in particular if addressed specifically to a child, and shall be clearly distinguishable from other information.*** ***2b. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the right to object may be exercised by automated means using a technical standard which allows the data subject to clearly express his or her wishes.*** ***3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned for the purposes determined in the objection.*** (38)… Legitimate interest could exist for example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. iIn particular where such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests.

Council's amendments	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child. **Article 8** 1. Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child is given by the child in circumstances where it is treated as valid by Union or Member State law. 1a. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. **Article 11 is deleted** **Article 12** The controller shall take appropriate measures to provide any information referred to in Articles 14 and 14a and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, where appropriate electronically. Where the data subject makes the request in electronic form, the information may as a rule be provided in electronic form, unless otherwise requested by the data subject. When requested by the data subject, the information may be given orally provided that the identity of the data subject is proven.
Trilogue	Information is not available

Opinions of Article 29 WP and EPDS

Title of a document	**Text**	**Summary/Key Points**
Article 29 WP, Working document on biometrics, 12168/02/EN WP 80, 2003	A specific concern related to biometric data is that the public may become desensitised, through the widening of the use of such data, to the effect their processing may have on daily life. For example, the use of biometrics in school libraries can make children less aware of the data protection risks that may impact	Risks of becoming "desensitised". Portuguese and German DPAs are reluctant to accept the use of biometric data of

	upon them in later life. The use of biometrics additionally raises the issue of proportionality of each category of processed data in the light of the purpose for which the data are processed. Biometric data may only be used if adequate, relevant and not excessive. This implies a strict assessment of the necessity and proportionality of the processed data18. For instance, the French CNIL has refused the use of fingerprints in the case of access by children to a school restaurant,19 but accepted for the same purpose the use of the outline of the hand pattern. The Portuguese data protection authority has recently issued an unfavourable decision concerning the use of a biometric system (fingerprint) by a university to control the assiduity and punctuality of the non-teaching staff20. The German data protection authority has handed down a favourable decision on the introduction of biometric characteristics on identity papers in order to prevent their falsification, provided that the data are stored in the microchip of the card rather than in a database for comparison with the owner's fingerprints.	children and employees.
Article 29 WP, Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of	4. Processing of Biometric Data The current proposal provides that "Member States shall collect biometric identifiers comprising **the facial image and ten fingerprints from the applicant**… ", thus creating, as explained by the European Commission, the legal basis needed for the Member States to process the obligatory biometric identifiers of visa applicants. Given the potentially harmful consequences for the persons concerned, the use of biometric data for **identification purposes should be limited** and these data included in the VIS, as per the objectives of the VIS, only where absolutely necessary and subject to the relevant principles and guarantees. This is all the more important in the case of groups especially at risk, such as children and the elderly. _ c1) Age of visa applicants The age under which children will **be exempted from the obligation to provide fingerprints is set at 6**, with no maximum age set for elderly people. These important provisions are set out in the CCI regulation and dealt with as a purely technical issue whereas they should form the basis of a broader policy debate. The inclusion of a reference to the Convention on the Rights	As regards children and the elderly, the collection and processing of fingerprints should be restricted and the age limits made consistent with the age limits in place for other large EU biometric databases (such as Eurodac). EURODOC - The Eurodac system enables European Union countries to help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union: age limit 14 VIS Regulation- short-stay visa: age limit 12 (Article 13.7)

visa applications (COM(2006)269 final), WP 134, 2007	of the Child must be regarded as a precondition for assessing **respect for children's dignity in connection with the said obligation** – i.e. it should not be regarded as a merely administrative reference standard in the enrolment procedure. The WP takes the view that – for the sake of the person's dignity and to ensure reliability of the procedure – the collection and processing of fingerprints should be restricted for children and for elderly people and that the age limit should be consistent with the age limits in place for other large EU biometric databases (Eurodac, in particular). It must be taken into account that there is no scientific literature giving conclusive evidence that the fingerprinting technology is sufficiently reliable when it concerns either children or the elderly. The error range that can be guaranteed by manufacturers with regard to the fingerprints stored in the system (for 5 years) and the controls (hit/no hit) to be carried out in the five years (or 48 months) during which those fingerprints are kept should also be established. This applies, in particular, to children under a given age and to other individuals with specific diseases and/or progressively deteriorating conditions – **as the likelihood of a mismatch increases with time in such cases**. The procedures to ensure respect for human dignity and fundamental freedoms should be also specified in these cases. Given the lack of studies on this point and of explicit certification by manufacturers concerning the stability and quality levels that can ensure reliable matches with C-VIS fingerprints related to children under and/or elderly people over a given age, the WP considers that laying down new, different age limits for exemption from fingerprinting is not justified, that it impinges on the data subject's dignity, and that it is unnecessary in view of the low risk associated with the above categories and the purposes for which the VIS was set up. Since the draft provides for fingerprints to be taken for the ten fingers of the applicant's hands, which unquestionably ensures high quality in terms of identification, it is worth recalling that – under the criterion in place with regard to entering fingerprint data in Eurodac - Eurodac only stores fingerprints of persons **at least 14 years** old and no older than 80. The fragility of fingerprints makes it preferable to collect them exclusively for the purposes of verifying a person's identity, without prejudice to the possibility of collecting such data (in accordance with the mechanisms and safeguards set out under domestic	

	law) wherever this is necessary, for instance, to prevent identity theft. In particular, the unreliable **fingerprint data of children under the age of 14 cannot be used for identification purposes**, and therefore access to data provided for identification purposes under Article 17 of the VIS proposal for a Regulation cannot be authorised; this must be explicitly stated. –	
Article 29 WP, Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), 2008	Biometric data – access to the school and canteen Over the years, there has been an increase in access control in schools. This access control may involve collecting, at entry, biometric data such as fingerprints, iris, or hand contours. In certain situations such means may be disproportionate to the goal, producing an effect which is too intrusive. In any case, the proportionality principle should be applied to the use of these biometric means as well. It is strongly recommended that legal representatives have available to them a simple means of objecting to the use of their children's biometric data. If their right to object is exercised, their children should be given a card or other means to access the school premises concerned.	
Article 29 WP, Opinion 3/2012 on developments in biometric technologies, WP 193, 2012	**Consent & Transparency**: Consent is a core issue in the use of fingerprints for uses other than in law enforcement. Fingerprints can be easily copied from latent prints and even photographs without the individual's knowledge. Other issues concerning **consent are those related to obtaining child's consent and the role played by parents in this regard (e.g. for fingerprinting in schools)** as well as the validity of consent for providing fingerprints in a labour context. 3.7. **Safeguards** for people with **special needs** The use of biometrics could impact significantly on the dignity, privacy and the right to data protection of **vulnerable people** such as **young children, elderly people and persons physically unable to complete the enrolment process successfully.** Given the potentially harmful consequences for the persons concerned, more stringent requirements will have to be met in the impact assessment process of any measure interfering with an individual's dignity in terms of questioning the necessity and proportionality as well as the possibilities of the individual to exercise his right to data protection in order for that measure to be deemed admissible.	It is recommended not to process biometric data of children younger than 14 years. Measures against stigmatization or discrimination.

	Appropriate safeguards must be in place against the risks of stigmatization or discrimination of those individuals either because of their age or because of their inability to enrol. Regarding the introduction of a generalized legal obligation of collecting biometric identifiers for these groups, notably, for young children and elderly people at border controls for identification purposes, the Working Party has taken the view that – "for the sake of the person's dignity and to ensure reliability of the procedure – the collection and processing of **fingerprints should be restricted for children and for elderly people and that the age limit should be consistent with the age limits in place for other large EU biometric databases (Eurodac, in particular)**." 10 In any case, specific safeguards (such as appropriate fall-back procedures) should be implemented so as to ensure the respect for human dignity and fundamental freedoms of any individual that is unable to complete the enrolment process successfully and thereby avoid burdening such individual with the imperfections of the technical system 11. – Examples of AFIS at EU level are Eurodac and the Visa Information System that - according to the expectations - will be among the largest databases in the world considering that approximately 70 million fingerprints will be stored in those systems. In its previous opinions the Working Party raised several questions on the use of large scale databases considering the need to ensure proportionality. **Especially reliability problems in terms of false-positive and false-negative findings, effective access control to these databases and problems related to the use of fingerprints of children and elderly people need to be addressed.** Templates are commonly used in biometric systems based on fingerprinting and are usually considered by system providers as a way to protect the individual. Nevertheless, depending on the system / algorithm used to generate the template, there are potential risks related to the possibility to link templates with other fingerprint databases in order to identify individuals. The use of systems to circumvent fingerprint recognition systems by using artificial fingers or fingerprints made from artificial material allowing identity theft practices is also a relevant issue. There are different approaches to reduce the vulnerability of these systems such as live detection, systems based on	

	the recognition of multiple fingers and also the use of adequate human supervision for enrolment and identifications / verification tasks. _ In a kindergarten a vein pattern scanner is installed to check every adult person entering (parents and members of staff) whether they are entitled to enter or not. To run such a system the storage of fingerprints of all parents and staff members would be required. Consent would be a questionable legal basis especially for the employees as they might not have a real choice to refuse the use of such a system. It would be **questionable for the parents too as long as there is no alternative method to enter** the kindergarten.	
EDPS, Opinion No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 2008	The case of children 11. In the explanatory memorandum of the proposal, the Commission refers to pilot projects in some Member States which have underlined that fingerprints from '**children under the age of 6 seemed not to be of a sufficient quality for one-to-one verification of identity**'. However, little or no information is available on these pilots and the circumstances in which they have been conducted; what 'sufficient quality' means has been neither explained nor defined until now. 12. According to the EDPS, the age limit for children in giving fingerprints should be defined by a consistent and in-depth study which is to identify properly the accuracy of the systems obtained under real conditions, and which is to reflect the diversity of the data processed. The pilot projects as such do not provide sufficient information on which fundamental choices of the Community legislator can be based. 13. The EDPS already underlined the need for such a study prior to any age limit definition in his opinion (6) on the proposal for a Regulation amending the Common Consular Instructions. Neither the available scientific literature nor the previous impact study conducted by the Commission in the frame of the Visa Information System proposal (7) presented conclusive evidence on a solidly based age limit for children. 14. The EDPS recommends therefore that the age limit selected in the proposal should be considered as a provisional one. After three years, the age limit should be reviewed and supported by a large scale and in-depth study. Considering the sensitiveness of biometric data, as well as the competitive dimension of biometric systems, the EDPS suggests that this study should benefit from the	

	management of a single European institution which has clear expertise and test-bed facilities in this field (8). All relevant stakeholders from industry to member states authorities should be invited to contribute to the study. . Before the age limit is clearly defined by this study and in order to avoid any hazardous implementation, the EDPS recommends that the applied limit corresponds to those already adopted for large populations in the Regulation on the Eurodac system (9) related to the asylum seekers **(the age limit for collecting children's fingerprints is 14 years**) or the US Visit programme (10) (also 14 year age limit). These limits could be even slightly lower as the use of biometric data is strictly limited to a verification process (one to one comparison) according to Article 4(3) of Regulation (EC) No 2252/2004. Indeed, fewer errors are usually produced by such a process compared to an identification process (1 to n comparison) which presents higher error rates.	

Country studies

Country, Title, online source	Text	Summary
UK: Protection of Freedoms Act 2012, section 26-27	***Requirement to notify and obtain consent before processing biometric information*** (1)This section applies in relation to any processing of a child's biometric information by or on behalf of the relevant authority of— (a)a school, (b)a 16 to 19 Academy, or (c)a further education institution. (2)Before the first processing of a child's biometric information on or after the coming into force of subsection (3), the relevant authority must notify each parent of the child— (a)of its intention to process the child's biometric information, and (b)that the parent may object at any time to the processing of the information. (3)The relevant authority must ensure that a child's biometric information is not processed unless— (a)at least one parent of the child consents to the information being processed, and (b)no parent of the child has withdrawn his or her consent, or otherwise objected, to the information	Legal framework

	being processed. (4)Section 27 makes further provision about the requirement to notify parents and the obtaining and withdrawal of consent (including when notification and consent are not required). (5)But if, at any time, the child— (a)refuses to participate in, or continue to participate in, anything that involves the processing of the child's biometric information, or (b)otherwise objects to the processing of that information, the relevant authority must ensure that the information is not processed, irrespective of any consent given by a parent of the child under subsection (3). (6)Subsection (7) applies in relation to any child whose biometric information, by virtue of this section, may not be processed. (7)The relevant authority must ensure that reasonable alternative means are available by which the child may do, or be subject to, anything which the child would have been able to do, or be subject to, had the child's biometric information been processed. ***27. Exceptions and further provision about consent and notification*** (1)For the purposes of section 26(2) and (3), the relevant authority is not required to notify a parent, or obtain the consent of a parent, if the relevant authority is satisfied that— (a)the parent cannot be found, (b)the parent lacks capacity (within the meaning of the Mental Capacity Act 2005) to object or (as the case may be) consent to the processing of the child's biometric information, (c)the welfare of the child requires that the parent is not contacted, or (d)it is otherwise not reasonably practicable to notify the parent or (as the case may be) obtain the consent of the parent. (2)A notification under section 26(2) must be given in writing, and any objection to the processing of a child's biometric information must be made in writing. (3)Consent under section 26(3) may be withdrawn at any time. (4)Consent under section 26(3) must be given, and (if withdrawn) withdrawn, in writing. (5)Section 26 and this section are in addition to the	

	requirements of the Data Protection Act 1998.	
UK: ICO Issues paper, Protecting Children's Personal Information	The Information Commissioner recognises the difficulties involved **in judging whether a child is capable of giving fully informed consent, and he would always recommend as good practice that parents should be consulted about important decisions affecting their children**. Nevertheless, it must be emphasised that the Data Protection Act 1998 confers rights on the Data Subject, i.e. the child. These rights should only be exercised by another on their behalf if they are not capable of exercising them independently. Given the continued development of case law touching upon **the autonomy of a child**, the Commissioner believes that the time may be right for him to issue further guidance in the context of data protection rights and obligations. The ICO will be reviewing what it can do to provide a clearer steer for those having to deal with difficult practical decisions. However**, consent will not always be the only way to ensure fair and lawful processing. Indeed, given the difficult issues that have been mentioned, it may be safer for data controllers to rely on another basis for the processing.** It is certainly not the intention of the Data Protection Act to deprive children of protection where parents unreasonably refuse their consent. It is also important that the seeking of consent is not undertaken on an inappropriate basis such as where processing is likely to go ahead with or without consent.	Always consult parents
UK: ICO, Personal information online code of practice, https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf	By '**vulnerable people'** we mean individuals who, for whatever reason, **may find it difficult to understand how their information is used**. This could be because they are children, have a learning disability or lack technological understanding. Data protection law says that you have to process personal data fairly. This duty applies regardless of the level of understanding of the people you collect information from. You should try to **assess the level of understanding** of the people your service is aimed at and must not exploit any lack of understanding on their part. One of the difficulties of providing services online is that very often you will not know: • who is accessing your service; • how old they are; • what their level of understanding is; • how 'internet savvy' they are; or • whether they have a disability that affects their understanding. Even if you collect reliable 'real world' identifiers, such as names and dates of birth, this still doesn't mean you can judge	

	levels of understanding reliably. People could provide false details in order to access services. For example, a child could lie about their age. Uncertainty over the 'real world' identity and characteristics of those you are dealing with does not mean that you cannot collect personal information about them. However, if your website is targeted at a particular group, for example children, there are some precautions that you should take. The adoption of good practice will help to ensure that you handle the personal data of all those that use your services fairly, but it is especially important when dealing with people who are particularly vulnerable or lack understanding. Information about children There are many difficulties when collecting information from children, including **determining whether parental consent to data collection should be obtained and, if so, what form it should tak**e. For example: • In the UK there is no simple legal definition of a child based on age. Even if there was, you might not know the ages of many of the individuals you are dealing with, or be able to rely on the information provided by the child or "adult" as to age. • **Children of a similar age can have different levels of maturity and understanding**. Consideration of these attributes, as well as age, will be required to ensure that children's data is processed fairly. • A resourceful and determined child could circumvent many mechanisms for obtaining his or her parent's consent for the collection of personal data. Age and understanding Assessing understanding, rather then merely determining age, is the key to ensuring that personal data about children is collected and used fairly. Some form of parental consent would normally be required before collecting personal data from children under 12. You will need to look at the appropriate form for obtaining consent based on any risk posed to the child. You may even decide to obtain parental consent for children aged over 12 where there is greater risk. This has to be determined on a case by case basis. Other laws, industry rules or codes of practice may apply to your organisation, for example, restrictions on targeting direct marketing at children under a certain age. It is clear that certain services are aimed at particular age groups, for example children of primary	

	school age or those in their early teens. It is good practice for the providers of such services to ensure that they only collect personal data in a way that their core audience is likely to understand and that their parents would be unlikely to object to if they knew about it. In short, this means that as complexity increases, it will become more likely that only an older child will have the necessary understanding. Parental consent It is good practice to seek parental consent if the collection or use of information about a child is likely to result in: • disclosure of a child's name and address to a third party, for example as part of the terms and conditions of a competition entry; • use of a child's contact details for marketing purposes; • publication of a child's image on a website that anyone can see; • making a child's contact details publicly available; or • the collection of personal data about third parties, for example where a child is asked to provide information about his or her family members or friends. This excludes parents' contact details provided for the purpose of obtaining parental consent. The key issue is **to take into account the degree of risk that the collection or use of the personal data poses to the child or to others.** This will help you to determine whether parental consent is required and, if so, what form this should take. For example, where minimal information is being collected, such as an email address to register on a site and to ask the child to confirm their age, then asking the child to tick a box to confirm parental consent and sending an email to the parent may be sufficient. However, if the child's photo is to be displayed on a website, you may require a signed consent form or email acknowledgement from the parent even for older children. Obtaining reliable parental consent can be very difficult. One problem is that it is often the child accessing the service that will be asked to provide their parents' details. This could allow the child to provide false parental details, for example by setting up a bogus email contact address. The promise of a prize or other inducement could encourage resourceful children to do this.	
UK: Education Department, Protection of Biometric Information of	**Are schools required to ask/tell parents before introducing an automated biometric recognition system?** Schools are not required by law to consult parents before installing an automated biometric recognition	

Children in Schools	system. However, they are required to notify parents and secure consent from at least one parent before biometric data is obtained or used for the purposes of such a system. It is up to schools to consider whether it is appropriate to consult parents and pupils in advance of introducing such a system. • Schools and colleges must ensure that each parent of a child is notified of the school's intention to use the child's biometric data (see 1 below) as part of an automated biometric recognition system. • The written consent of at least one parent must be obtained before the data are taken from the child and used (i.e. 'processed' – see 3 below). This applies to all pupils in schools and colleges under the age of 18. In no circumstances can a child's biometric data be processed without written consent. • Schools and colleges must not process the biometric data of a pupil (under 18 years of age) where: a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data; b) no parent has consented in writing to the processing; or c) a parent has objected in writing to such processing, even if another parent has given written consent. • Schools and colleges must provide reasonable alternative means of accessing services for those pupil. Notification sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. This should include: details about the type of biometric information to be taken; how it will be used; the parents' and the pupil's right to refuse or withdraw their consent; and the school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed.	
UK: Biometric Technologies in Schools Draft Guidance for Education Authorities:	"Section 1.2 States clearly that the use of biometric systems in schools is a decision for education authorities to make. It informs authorities of good practice to be followed in implementing such systems. It asks if there is an identified need for such technologies and lists as key issues, the question of	Decision of education authorities

Consultation Analysis Report February 2009	consent by users and their parents including the right to opt out without penalties" (Wester Cleddens Primary School, School Board)	
Belgium: DPA Comments on DP reform	An age-based definition has the advantage of legal certainty. Still, the CPP is of the opinion that the random determination of age (age of majority) with respect to the protection of personal data is difficult to reconcile with the reality of use, for example of the internet, by (sometimes very) young people. In analogy to what has been provided in recommendation Rec (2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes the CPP either recommends informing, consulting children and taking into account their desires from a certain age or gradually involving them in the decisions that have to be taken for example with respect to the exercise of their rights, depending on their power of judgment. This approach reflects the CPP's aim of encouraging young people to adopt a well-informed, responsible and respectful (of themselves and others) attitude when using information and communication technologies18 . **The CPP shares the desire of the European Commission to subject large databases concerning minors to a prior data protection impact assessment** (article 33),	Belgian DPA support age limit of 12 and 14
Spain: The Organic Law 15/1999 relating to Personal Data Protection (Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal) (the "DPA") implemented the Data Protection Directive. The DPA has been further developed by Royal Decree	***Royal Decree 1720/2007,*** RTICLE 13. CONSENT FOR THE PROCESSING OF DATA OF MINORS. 1. Data pertaining to data subjects over fourteen years of age may be processed with their consent, except in those cases where the law requires the assistance of parents or guardians in the provision of such data. The consent of parents or guardians shall be required for children under fourteen years old. 2. Under no circumstances may data be collected from the minor regarding information about any other member of the family unit, or about its characteristics, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refer. The aforesaid notwithstanding, data regarding the identity and address of the father, mother or guardian may be collected for the sole purpose of obtaining the authorisation set out in the previous subsection. 3. When processing refers to the	In Spain, the data protection legislation explicitly states that personal data of over 14 year olds may be processed with their consent, except 'in those cases where the law requires the assistance of parents or guardians in the provision of such data'. The general rule of thumb in Denmark seems to apply the age of legal competency (15) to data protection as well. The DPA, however, has stressed that this is merely a rule of thumb and that all relevant elements in each particular situation should be taken into account. In

1720/2007	data of minors, the information aimed at them shall be expressed in easily understandable language, with express indication of the provisions of this Article. 4. The data controller is responsible for setting up the procedures that guarantee that the age of the minor and authenticity of the consent given by the parents, guardians or legal representatives have been effectively checked.	Sweden there is a similar guideline (age of 14-15, exceptionally 13) that remains subject to context-specific elements and the minor's level of maturity.
Spain: Derechos de niños y niñas - Deberes de padres y madres: Guía de recomendaciones 2008, DPA handbook on processing children's	**If the child is under 14 their data cannot be processed without the consent of mothers, fathers or legal guardians.** Children over 14 will be entitled to give their own consent. When our consent is requested for any activity of a minor over 14, it should also be requested for processing the child's data. Duty to inform the children People processing the data of minors must inform them of this in such a way as may be intelligible to them. We should make sure that they are informed of the identity of the processor, the purpose and uses for which the data is requested, whether this data will be communicated or transferred to third parties and whether or not it is obligatory to provide the data. The processors must also furnish an address for exercising the rights of access, rectification, erasure and objection. Our authorisation is needed The data of our children under 14 cannot be processed without first asking for our consent. To do so, data processors must present us with a written document or any other medium through which they seek our consent for the intended purpose. They must also request documents that vouch for our status as parent or legal guardian. We should also be aware of the fact that this consent we have freely given for our children's data to be processed can just as freely be withdrawn afterwards. Use of the data must be proportional Data can be processed only for the purpose it was collected. Furthermore, no more data than that which is strictly necessary for this purpose in view may be requested. People processing the data of our children are required to keep this information safe and ensure it is up to date. They may not use this information for any other purpose and must guarantee the security and secrecy. They will also cancel the data when it is no longer necessary	
France: Visa to France information	For the 12-years-old: personal attendance of every applicant is compulsory when they submit their visa application at VFS Centre. Indeed, and for persons who	

	are 12 years old, finger prints must be collected. **Minors between the ages of 12 and 18: they must be accompanied by one of their parents or by the legal tutor.** Children under 12 years of age: they do not need to attend VFS appointment as they are exempted from biometrics. Moreover, and for security reasons, they are not allowed to enter VFS Centre.	
Poland: Passport information, 0-13	A child who has not turned 5 will be issued a temporary passport that will be valid for 1 year. In exceptional situations, at the written request of the parents, this child can be issued a passport (biometric) that will be valid for 1 years.	
Sweden: DPA requirements	Protection of Minors The protection of minors is not specifically mentioned in the PUL. However, the Data Inspection Board has found that the use of personal information of children under the age of 13 requires consent from the parent of the child.[22] It is thus not sufficient that a child under 13 consents to the treatment of his or her personal information.	
Lithuania: implementing rules	In Lithuania the head of the school has to approve the processing of additional data related to a child such as address, telephone number of parents, guardians, and their names	
Germany: school councils	e.g., http://www.schulamt-aic.de/html/datenschutz.html	
Ireland:	https://www.dataprotection.ie/docs/Biometrics-in-Schools-Colleges-and-other-Educational-Institutions/409.htm The Commissioner considers that use of a minor?s personal data cannot be legitimate unless accompanied by the clear signed consent of the child and of the child?s parents or guardian.	
USA: information on use biometrics at school	Maryland - SB855, Feb 2013, Public Schools – Collection of Biometric Information from Students Prohibited - Halted in the House Ways and Means Committee, May 2013. Arizona SB1216 - July 2008, Consent using biometric technology in schools Illinios SB1702 - 2007, Consent using biometric technology in schools Illinios HB1559 - School Code amended. Re: biometric	Regulation varies in different states; in some states it is prohibited

	consent Illinois SB2549 - 2005/2006, Consent using biometric technology in schools	
New Zeeland: Collection and Handling of Biometrics at the Ministry of Business, Innovation, and Employment IMMIGRATION NEW ZEALAND IDENTITY AND BIOMETRICS PROGRAMME P	Consideration of end users The fourth guiding principle recommends that end users of any business process that includes biometrics should be appropriately consulted. That consultation should include social and cultural considerations, accessibility issues (if relevant) or other constraints or concerns. These concerns and constraints should inform the type of biometrics to be used or inform the development of requirements for implementation. Information to end users and consultation with end users and stakeholders As described above, the consultation process undertaken in April 2006 incorporated a variety of external stakeholders and people affected by the collection and handling of biometric information. Many submitters commented on the safeguards that needed to be addressed in the legislation. Submitters commented that the legislation should be consistent with privacy and human rights legislation and include provisions on: • the uses to which the information must be put • the length of time that information is stored and the means by which it must be stored • the circumstances under which information may be shared with other governments and other government Ministries • the means by which people can access and, if necessary, correct their personal information • a process for reviewing the handling and use of biometric information.	

Documents on consulting children

	Consultation with children & young people: toolkit	This is a practical guide about how to consult with children and young people on policy related issues. It is written for community workers, youth workers, teachers, local authority workers,

		facilitators and other organisations and individuals working with children and young people
2007	Consultation with children and young people	An example of consultation
	Consultation with children & young people: Toolkit	

Popular media

Title
RT link here Jan. 11th 2014 : UK schools fingerprinted over 800K children, third without parental consent - watchdog
Privacy Protection for Minors…? – an overview of consent practices for children's consent

1.2.2 Employees

1.1.1.1 Introduction to the legal framework applicable to the processing of employees' data

At the international level, Article 8 of the European Convention on Human Rights and Fundamental Freedoms provides the right to respect for private life, which is also applicable for the employees. In order to consider whether the right to respect for one's *"private and family life, his home and his correspondence"*, covers as well the aspects of one's professional life, the case law of the European Court of Human Rights must be taken into consideration[47]. From this case law, it has been well established that in order to strike a balance between the interest of employers to have in place an efficient security mechanism and the right to respect their employees' privacy, the following safeguards should be taken into consideration. In a case by case approach, it must be examined if there is an interference with one's right to respect for privacy when introducing a security mechanism, and in an affirmative answer, it should be examined if this interference is in accordance with a law, which must be foreseeable, accessible and specific. Also, it must be assured that this interference pursues a legitimate aim, necessary in order to achieve the aimed purpose and that there is no other less intrusive way for achieving this purpose.

Moreover, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No 108), provides the general safeguards for reconciling the fundamental values of the respect for privacy and the free flow of information between people, while the Draft Recommendation on the processing of personal data in the context of employment includes specific provisions and safeguards regarding the processing of employees' personal data. Regarding the employees' biometric data, the draft recommendation provides that the collection and further processing of the employees' biometric data should only be undertaken when it is necessary to protect the legitimate interests of employers, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards. The latter would be to provide up to date information to the employees in a transparent manner before the introduction of information systems and technologies about the purpose of the operation, the

preservation or back-up period, as well as the existence or not of the rights of access and rectification and the way to exercise them. Moreover, employers should have in place appropriate internal procedures relating to the processing of that data and consult the employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change, as well as consult, in accordance with domestic law, the national supervisory authority on the processing of personal data.

At the European level, the relevant legal framework is set forth by the Data Protection Directive 95/46/EC, which is transposed to national laws implementing the Directive. National laws foresee diverse requirements for the processing of employees' personal data, for example, in France, the use of access control, will be subject to information and consultation with the employees' representatives in the company. Consulting stakeholders, such as the employees' representatives, work councils and/or trade unions, is not mandatory by the current data protection framework, but is required by several national legislations (e.g. French Labour Code L2323-32) and Laws No. 84-16 of January 11, 1984, No. 84-53 of January 26, 1984 and No. 86-33 of January 9, 1986). This requirement also aligns with the provisions of the Draft Recommendation on the processing of personal data in the context of employment (Article 21) of the Council of Europe.

The proposed upcoming General Data Protection Regulation reconfirms the above mentioned country-specific regulations relating to employees' personal data (Article 82 of GDPR). Therefore, prior to developing an information system that would process employees' personal data, an entity should consult the applicable national legislative framework. Also, regarding stakeholders' consultation, there are several provisions in the proposed GDPR providing for the transparency requirement, enhancing the employees' empowerment in the decision-making process (Articles 11, 43 1 (a) etc of the proposed GDPR), while simultaneously taking into consideration the ad hoc applicable national legislation.

1.1.1.2 Recommendations for consulting stakeholders on information systems employees' biometric data

When consulting stakeholders about an information system that will process employees' biometric data, controllers are recommended to:

1. Identify the relevant stakeholders of the information system that will process the employees' biometric data.

a. Consultation with the different stakeholders affected by the system; employees and/or the employees' representatives (work councils, trade unions).

b. For the identification of the relevant stakeholders, the applicable national legislation must be taken into consideration. For instance, in France, pursuant to the provisions of the Labour Code (L2323-32) and according to Laws No. 84-16 of January 11, 1984, No. 84-53 of January 26, 1984 and No. 86-33 of January 9, 1986, the employees' representatives must be consulted and informed of any envisaged mechanisms implementing functionalities able to affect the employees. In addition, the French Labour Code provides that

no information concerning directly an employee can be collected by a device that has not been previously brought to his/her attention (L1221-9 and L1222-4).

2. Provide all relevant information related to the processing of employees' biometric data.

a. The information of the employees should concern the collection, use, disclosure, access, correction, retention and disposal of their personal information, including all administrative, physical and technological security controls and compliance put in place (Article 14 of GDPR). In particular, the communicated information should include the purposes for which the biometric data would be processed (e.g. working time management purposes), the legitimate interests of the data controller to collect biometric data; the (preliminary) proportionality analysis, the period for which the personal data would be stored; the possibility to object to the processing; where applicable, information about the existence of profiling, or measures based on profiling, and the envisaged effects of profiling on employees; and meaningful information about the logic involved in any automated processing

b. Provide information about the privacy risks analysis performed and explain the reasons that motivated these choices. Such reasons could include information about the nature of the risk identified, why you considered this to be a risk, the interests at stake and the measures taken to reduce this risk.

c. Ensure that the notification is complete, clear and appropriate to the target audience based on the nature of the personal data and the practical means chosen (Article 12 of GDPR).

3. Collect and record information provided by employees and other stakeholders on the proposed system.

a. Information provided by employees and their representatives may include comments, ideas, concerns and other input. To ensure accountability of the decision-making process it is important that this information is properly documented.

b. Obtaining personal data from employees, requires prior consultation with their representatives in several Member States, such as France.

c. Consider techniques to analyse the received information.

4. Question stakeholders about potential risks and alternative solutions to the proposed system.

a. Stakeholders are able to better identify risks and foresee alternative solutions to the proposed system.

b. Alternative and/or less intrusive solutions should be provided in case the employees or their representatives object to the processing of their biometric data. For instance, in a case about access control of authorized users to company sites and systems the Hellenic DPA in its Decision No 74/2009, considered as unlawful the processing of biometrics, since the control of entry into the company could be achieved by less restrictive means, such as access cards without biometrics and that special security measures should be taken only for accessing specific sites and software applications (server room, store documents, etc.).

5. Ensure accountable and objective decision making process.

a. Since consultation is a part of the Privacy Impact Assessment, a careful balance between all relevant parties, in respect of the proportionality principle, is required.

b. Involving employees and/or their representatives in the decision-making process, enhances the employees awareness and is aligned with the transparency requirement (Articles 11, 43 1 (a) etc of the proposed GDPR).

6. Communicate the findings of the consultation process to employees and all relevant parties.

a. Following the consultation's findings, data controllers should explain how the received comments have been incorporated into the design of the system.

Methodology

To prepare the above-mentioned recommendations, a desk-research was carried out, taking into account the following:

6. Relevant provisions of 95/47/EC Directive, as well as upcoming changes in the proposed GDPR on information notice, consent, and PIA.
7. Opinions of Article 29 WP and EDPS on information notice, consent, and biometric data.
8. National DPA's Opinions and national case law on the processing of employees' biometric data.
9. Other media (e.g., blog posts, news reports, etc).

Key words: employees, biometric data, consent, consultation, PIA.

Legal framework

Institution	GDPR text
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdfCommission's proposal 2012	**Article 4 (11)** "biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;.." **Article 11** "Transparent information and communication 1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights." **Article 33.2 (d)** "1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope

	or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. 2. The following processing operations in particular present specific risks referred to in paragraph 1: (d) personal data in large scale filing systems on children, genetic data or biometric data." **Article 43 (1) (a)** "..(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;" **Article 82** "Processing in the employment context 1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship."
Parliament's amendments 2014	**Article 4 (11)** "'biometric data' means any

	personal data relating to the physical, physiological or behavioural characteristics of an individual which allow his or her unique identification, such as facial images, or dactyloscopic data;..” **Article 11** “Transparent information and communication 1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.” **Article 37 (1) (j)** Tasks of the data protection officer “…to inform the employee representatives on data processing of the employee***..”.*** **Article (43) (1a)** “With regard to employment data, the representatives of the employees shall be informed about and, in accordance with Union or Member State law and practice, be involved in the drawing-up of binding corporate rules pursuant to Article 43.” **Article 82** Minimum standards for processing data in the employment context “1. Within the limits of this Regulation, Member States may, in accordance with the rules set out in this Regulation, and taking into account the principle of proportionality, adopt by law legal provisions specific rules regulating the processing of employees' personal data in the employment context, in particular for but not limited to the purposes of the recruitment and job applications within the

	group of undertakings, the performance of the contract of employment, including discharge of obligations laid down by law or and by collective agreements, in accordance with national law and practice, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. Member States may allow for collective agreements to further specify the provisions set out in this Article."
Council's amendments July 2015	**Article 4 (11)** "'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the their unique identification of that individual, such as facial images, or dactyloscopic data" **Article 82** "Member States may adopt by law specific rules or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality

	and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
Modernisation proposals of Convention 108 of the Council of Europe	**Article 6** "the processing of genetic data, of personal data concerning offences, criminal convictions and related security measures, the processing of biometric data uniquely identifying a person, as well as the processing of personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where the applicable law provides appropriate safeguards, complementing those of the present Convention".

Opinions of Article 29 WP and EPDS

EDPS	Proposed definition for biometric data by EDPS reads as follows: "biometric data' means any personal data relating to the physical, physiological or behavioral characteristics of an individual which allow his or her unique identification, such as facial images, or dactyloscopic data".
Article 29 Working Party, Opinion 4/2007 (WP136), adopted on 20 June 2007 on biometric data	Biometric data may be defined as "biological properties, behavioral aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability."
Article 29 Working Party, Opinion 15/2011 on the definition of consent	The Article 29 Working Party stated clearly that where consent is required 'from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not

(WP187), adopted on Adopted on 13 July 2011 on employees' consent	consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice. An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid.

Country studies

Country	Legal framework
France http://www.cnil.fr/english/	Pursuant to the provisions of the Labour Code (L2323-32) and according to Laws No. 84-16 of January 11, 1984, No. 84-53 of January 26, 1984 and No. 86-33 of January 9, 1986, the employees' representatives must be consulted and informed of any envisaged mechanisms implementing functionalities able to affect the employees. In addition, the French Labour Code provides that no information concerning directly an employee can be collected by a device that has not been previously brought to his/her attention (L1221-9 and L1222-4).
Greece http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL	Law 2472/97 is implementing the Directive 95/46. Articles 2 par. 1, 5 par. 1, 9 par. 1, 25 par. 1 of the Civil Servants' Code concerning civil servants and employees of Legal Entities governed by Public Law, provide that this a refusal by the employees to process their biometric data will not constitute the cause of sanctions on behalf of the employers, since, in this way, the workers' personality is offended and this is considered as the manifestation of an act adversely affecting the labour contract.
Italy http://www.garanteprivacy.it/web/guest/home_en	Section 17 of the data protection Code (legislative decree no. 196/2003) concerning the processing of biometric personal data for the purpose of controlling employee assiduity at the workplace, provides that employees are alleged to be free to decide whether to participate in the assiduity control system based on biometric data, alternative measures being also available to any employees that are unable to have their assiduity recorded via the biometrics-based system because of physical reasons. Also, in order to verify compliance with working hours and simultaneously prevent unauthorised conduct by employees, the data controller can avail itself of other, less privacy-intrusive systems that do not impinge on personal freedom and do not involve an employee's body – which are both constituents of personal dignity, safeguarded by personal data protection provisions (Section 2 of the DP Code).
Belgium https://www.privacycommission.be/	In Belgium, since 01 April 2009, it is allowed to test employees on the work floor on drugs and alcohol for reasons of "prevention". This collective labor agreement describes various safeguards for the use of these tests in the employer-employee relation, which are gradually being introduced, because of the interference with the fundamental right to respect for privacy. Also, the Belgian Act of 2003 (Wet betreffende de medische onderzoeken die binnen het kader van de arbeidsverhoudingen worden uitgevoerd, 28.1.2003, B.S. 9.4.2003), allows 'biological tests', medical examinations or oral

	information collection 'with the aim to obtain medical information about the health condition or ascendants' only under strict and limited conditions in the employment context, requiring that such are relevant to the job and the medical condition required from the employee or the job applicant (see Article 3 §1), however, predictive genetic tests for employees and (for selecting) job applicants, are prohibited.

Case law

ECtHR	ECtHR 22 October 1981, No. 7525/76, Dudgeon v. the United Kingdom; ECtHR 15 May 1992, No. 15666/89, Kerkhoven and Hinke v. the Netherlands; ECtHR 16 December 1992 No. 13710/88, Niemietz v. Germany; ECtHR 25 March 1993, No. 13134/87, Costello-Roberts v. the United Kingdom; ECtHR 25 June 1997, No. 20605/92, Halford v. the United Kingdom; ECtHR 25 December 2001, No. 44787/98, P.G. and J.H. v. the United Kingdom, §56; ECtHR 28 April 2003, No. 44647/98, Peck v. the United Kingdom, §57.
France	-On 8 November 2007, CNIL reviewed for the first time five devices based on finger vein pattern recognition (VPR) designed to control access to premises or IT systems, reaching the conclusion that, in view of the current state of the art, vein pattern recognition is a traceless biometric process generating data that can be recorded in a database without any particular risks in terms of data protection. -Also, the Court had reviewed whether the purpose of the system to control the hours of employees working in public spaces of the train stations SNCF justified the use of a biometric system with centralized biometric data and since the controller did not demonstrate that the biometric application was the only means, the system was judged not proportionate to these purposes (see also CNIL's deliberations n°2005-031, n°2005-034, n°2005-035, 2005-036, 2005-037 of 17 February 2005, refusing the use of hand geometry for working time management purposes, deliberation n°2005-135 of 14 June 2005 authorizing the Hospital Centre of Hyères to use hand geometry for controlling the working time of employees and deliberation n°2006-101 of 27 April 2006, regarding the use of hand geometry for access control to professional premises, catering and working time management of employees). -Examples of refusing the deployment of a biometric system relying on fingerprint to control access: deliberations n°2007-254 of 13 September 2007, about refusing the deployment of a biometric system relying on the verification of fingerprint by the society Ecureuil Lease and deliberation n°2008-328 of 11 September 2008, about refusing the deployment of a biometric system relying on fingerprint to control access to certain areas of the "association hospitalière de l'Ouest", see also deliberation n°2005-113 of 7 June 2005, deliberation n°2007-256 of 13 September 2007 and deliberation n°2011-223 of 21 July 2011. -Examples of authorization are the following: deliberation n°2007-088, authorizing the central storage of fingerprint by the Casinos of Nivernais and La Baule to control access to the strong room and deliberation n°2007-080 of 25 April 2007 authorizing the Hospital of Strasbourg to deploy a biometric system

	relying on fingerprint to control access to operation rooms and deliberation n°2008-056 of 8 March 2008.
Greece	-Decision No 52/2003 of the Hellenic DPA is among the examples of decisions ruling as unlawful the processing of biometric data related to access control in security installations. More specifically, that case concerned the processing of employee's data to ensure their access to the Airport Business Center, by collecting and processing their biometric data, using the iris recognition technique. Interesting argument on the consent in the employment context: "7. Unnecessary personal data processing for the achievement of the purpose sought is not legitimate even when the data subject has given his/her consent according to article 5 par.1 or article 7 par. 2 section (a) of Law 2472/97 because the consent itself does not allow any act of processing contrary to the principle of purpose and necessity (decision no. 510/17/15.05.2000 of the Authority). As a result, consent does not quash the unlawful nature of the processing even when the data subject accepts exposure to biometric checks". -Another example provided from the Hellenic Data Protection Authority (No. 245/9/2000), relating to the legality of a control system for employees' access in the workplace, using the verification of fingerprints technique, in which the HDPA held that the processing of biometric data goes beyond the limits imposed by the principle of proportionality, in as much as the objective pursued can be achieved by milder means to control the presence of workers at work. -Also, with its Decision 56/2009, the Hellenic DPA permitted a certification service provider to establish a card-based fingerprinting biometric system for access control in the specific area used for the creation and maintenance of cryptographic keys (i.e. Certification Authorities' private keys used for signing the users' qualified certificates). -Similar was also the decision No. 9/2003 of the Hellenic DPA, concerning the access to the high security Athens Metro, where the Authority considered that the proposed biometric system is related to characteristics which leave no traces, but rather concern the geometry of the hand, a system consisted of devices that are autonomous with no link to the central database and other personal information, such as the name of the user, was not stored. -In its decision 74/2009, the Hellenic DPA considered as unlawful the processing of biometrics for the reason of access control to authorized users to company sites and systems. More specifically, in that case, the IT facilities of the company were in a room with an open-ended space, where anyone, after passing the main entrance, could gain access to company's activities related to critical data processing and software development secrets. The Authority held that control of entry into the space can be achieved by less restrictive means, such as access cards without biometrics, and that special security measures should be taken only for accessing specific sites and software applications (server room, store documents, electromechanical installations, etc.).
Italy	The Italian Data Protection Authority, in its Decision of July 21, 2005 has ruled on the use of fingerprints for assiduity control at the workplace. More specifically, this case concerned a manufacturing company, which lodged a request for prior checking about the processing of biometric data related to the its employees with a view to controlling their assiduity at work and thereby allocating standard and

	overtime pay. Operation of the above system would require the preliminary collection of biometric data (so-called enrolment phase), whereby the company would turn the image of part of the employee's fingerprint into a digital code using electronic devices equipped with both fingerprint readers and ad-hoc software; the said code would be assigned to each employee after being stored in the company's information system, without being encrypted or processed in any similar manner. The digital codes would be used as benchmarks for the digital codes obtained after reading (parts of) the employees' fingerprints whenever they leave and/or enter their workplace; such reading would be performed via readers located in several premises within the company, which would be connected with the company's information system. Due to lack of evidence that the requirements were met to ensure a high degree of reliability of the system in question and based on other grounds, the processing referred to in the submission was regarded as unlawful.

Other

Title
Irish Data Protection Commissioner's Office 'Biometrics in the Workplace' https://www.dataprotection.ie/viewdoc.asp?DocID=244
CNIL, Guide pour les employeurs et les salaries, 2010
Privacy and Data Protection Issues of Biometric Applications, Els J. Kindt, Faculty of Law – ICRI - KU Leuven

Annex 4: Designing the biometric system: questionnaire phase 2

Objectives

This second phase allows you to report all the necessary information regarding the characteristics and functioning of the biometric system. This information will then be compiled in order to generate a document summarizing such characteristics.

The questionnaire is divided into three categories of questions: enrollment, matching and security. Questions may be opened or closed.

1.1 Part 1/ Enrollment

1.1.1 Collection

1. Which biometric characteristics are processed?

Explanation: Biometric data are defined at European level as "biological properties, behavioral aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability."

☐ Fingerprint, ☐ Facial recognition; ☐ Voice recognition; ☐ Gait analysis; ☐ Signature recognition; ☐ Palm vein recognition; ☐ Finger vein recognition; ☐ Hand geometry; ☐ Iris ; ☐ Other

Explain

2. Is the choice of the type of biometric system the less intrusive with regard to the purpose(s) aimed at? Why?

Here, it is important to explain the reasons why the recourse to a given biometric technology or a combination of biometric technologies is the less intrusive option with regard to some other biometric technologies.

Explain

3. What are the data extracted from the biometric source?

Explanation: the amount of data extracted from a biometric source during the enrolment phase has to be adequate to the purpose of the processing and the level of performance of the

biometric system. The principle of data minimization means that only the required information and not all available information should be processed.

Explain briefly (e.g. number of fingerprints, number of finger vein patterns et cet…)

4. Aside from biometric data, what other categories(s) of personal data are you collecting during the enrollment phase?

Explanation: As a principle, the personal data processed must "not be excessive" in relation to the purposes for which they are collected. It commands that the controller shall collect only the personal data necessary to carry out the stated purposes of the processing. It is generally agreed that this principle of proportionality in relation to the "amount" of data collected must be understood as a principle of minimisation. Biometric systems that would require the collection and processing of other non biometric data for identity control purposes should assess strictly which kind of personal data are necessary to the system and limit the collection to such personal data.

Detail all personal data collected

5. How is the identity of the individuals to be enrolled checked?

Explanation: a particular attention should be paid to develop procedures that would ensure a reliable credential or identity check (E. Kindt "Best Practices for Privacy and Data Protection for the Processing of Personal Data" 351; J. Ashbourn "The Biometrics Constitution" 2012).

Explain

1.1.2 Transparency

6. How and at what time is enrollment carried out?

Explain briefly

Check the following conditions

☐ **The active participation of the individual is required**

Explanation: Whenever possible, enrolment requiring the personal involvement or active participation of the individual is to be preferred since it is more transparent and provides a suitable opportunity to provide information and fair processing notification. Any biometric system that would not require the active participation of the individual during the enrolment phase should be avoided.

Enrolment of people without their knowledge and/or consent, implying a covert collection, storage and processing of biometric data is as a principle, excluded. (the only exceptions admitted are very specific circumstances that fall outside the scope of the present impact assessment).

☐ **The individuals is provided with the necessary information in order to understand fully the reasons and implications of being enrolled in the biometric system**

Explanation: *The data controller should Ensure that individuals to be enrolled in the system receives sufficient information about the purposes and modalities of the system, as well as about their rights to ask for access and deletion of their data.*

Data subjects must be informed about the data processing activity and its purposes before or at the time their data are collected (Directive 95/46/EC Articles 10 & 11). The information notice that is communicated to data subject during the enrolment phase should contain the following items:

- *a description or visualisation of the matching procedure during which extracted bodyprints allow to identify a person (Biometrics Constitution);*
- *the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;*
- *the purposes of the processing for which the personal data are intended;*
- *the period for which the personal data will be stored;*
- *the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;*
- *in cases, where consent is required, provide a possibility to withdraw it;*
- *the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;*
- *the recipients or categories of recipients of the personal data, and conditions under which data may be transferred to the recipients (e.g., access to a video may be provided upon an official request of a law enforcement agency);*
- *where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;*
- *any further information necessary to guarantee fair processing in respect of the data subject (e.g., the procedure for the repudiation, under which conditions reenrolment procedure has to be repeated), having regard to the specific circumstances in which the personal data are collected;*
- *the level of security during all processing stages including transmission (e.g., over networks).*

1.1.3 Specific safeguards

7.	**Are they categories of people that are unable to enroll (young children, elderly people, persons physically unabled)?**

☐ **Yes**

☐ **No**

If yes

What are the appropriate safeguards (alternative procedure?) in place for people unable to complete the enrollment process?

Explanation: appropriate safeguards must be put in place against the risks of stigmatization or discrimination of those individuals either because of their age or because of their inability to enroll.

Detail

1.1.4 Biometric template protection

8. Do you satisfy essential conditions for the generation of the template?

Explanation: Following the Working Party 29 recommendations, key features can be extracted from the raw form of biometric data (e.g. facial measurements from an image) and stored for later processing rather than the raw data itself. This forms the biometric template of the data. The definition of the size (the quantity of information) of the template is a crucial issue. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions), on the other hand, the size of the template should not be too large so as to avoid the risks of biometric data reconstruction. The generation of the template should be a one way process, in that it should not be possible to regenerate the raw biometric data from the template.

☐ **Raw data are processed in order to extract biometric templates**

☐ **The size of the template is adequate to the purpose of the system**

Detail…

Is there any remaining risk of reconstruction of the raw data?

☐ No

☐ Yes

Explain the risks

☐ **The raw data are deleted after the template is generated**

Why is such storage considered most suitable compared to the storage on an individual device?

Detail…

1.1.5 **Retention**

9. How long is stored the biometric data and other personal data collected?

Explanation: The retention duration of biometric data should be assessed carefully. The data shall not be kept for longer than is necessary to achieve the stated purpose(s). This implies that once the data is not necessary anymore, it should be immediately deleted/erased. Also, each retention duration should be adapted to each category of data.

Detail each retention duration for each category of personal data and why such periods are considered necessary

10. Are they automated data erasure mechanisms in place to ensure that biometric data will not be stored for longer than necessary?

Explanation: in order to prevent that biometric information are stored for longer than is necessary for the purposes for which they were collected or subsequently processed, appropriate automated data erasure mechanisms have to be implemented also in case the retention period may be lawfully extended, assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system.

When using integrated storage on the reader, manufacturers may also implement storage of the biometric templates on volatile memory that guarantees that the data will be erased when the reader is unplugged. Therefore no biometric database remains when the reader is sold or uninstalled. Antipulling switches may also be used to automatically erase the data if someone tries to steal the reader.

Detail…

1.2 Part 2/ Matching

1.2.1 **Transparency**

11. When and how is matching carried out?

…

12. Is the active participation of the individual required?

Explanation: As it is the case during the enrollment phase, the active participation of the individual during the matching phase, whenever possible, constitutes a preferable option since it is a good opportunity for him/her to be aware of the processing of his/her biometric data. However, contrary to the enrolment phase, such participation may not always be possible.

☐ **Yes**
☐ **No**

If no, why?

In view of the above comment according to which the active participation of the individual is a preferable option, the process of matching without individual's active participation should be explained and duly justified.

…

1.2.2 Accuracy

13. What is the False Accept rate and False Reject Rate of the biometric system?

…

Why is this FAR and FRR acceptable considering the purpose of the system?

…

What is the alternative procedure of identity control in case of false reject rate?

…

1.2.3 Collection of matching information

14. Are data relating to matching operations registered? (e.g. date and time of identity control,)

Explanation: matching operations should only be retained if necessary to achieve the purposes for which the biometric access control system is justified (see answer to question 1).

☐ **No**
☐ **Yes**

If "yes"

For which purpose/further use matching operations are being registered by the system?

…

Are such purposes compatible with the original purpose of the biometric system (see answer question 1)

Explanation: Matching operations shall only be retained and further processed for purposes that are directly compatible with the original purposes for which a biometric access control system has been set up. (again see answer question 1).

Example: A biometric system set up to secure access to professional premises shall not be used to control the presence or working time of employees. These two purposes are distinct and cannot be considered compatible.

…

How long are matching information retained?

Explanation: The retention duration of matching operations should be assessed carefully. The data shall not be kept for longer than is necessary to achieve the purpose(s) for which matching operations are retained. This implies that once the data is not necessary anymore, it should be immediately deleted/erased. Also, each retention duration should be adapted to each category of data. Indefinite retention is in all cases prohibited.

…

Why is such retention period considered as necessary?

…

1.3 Part 3/ Security & accountability

The Working Party has identified technical and organizational measures aiming at mitigating data protection and privacy risks, that can help to prevent negative impacts. These technical measures aim in particular at mitigating the risks of identifty fraud, the risk of purpose diversion (or function creep) and the risk of data breach. Following the identification of the level of data

protection risks raised by a type of biometric, the organization should assess carefully the opportunity to recourse to some of the technical measures discussed in the questions below.

1.3.1 Data protection risks

15. According to the type of personal data and biometric characteristic collected and processed, what are the data protection risks associated with their use?

Explanation: It is important to identify the risks that are generally associated with such biometric system. The identification of such risks contributes to the understanding of the technology and its potential impacts on individual's rights. The identification of such risks is also a necessary step of any impact assessment. Risks should concern traditional security risks (confidentiality, integrity, availability) as well as privacy and biometric specific risks (identity theft, spoofing, impersonation, non repudiation, etc.).

Explain

1.3.2 Mitigating measures

16. Are all the locations of all personal data precisely identified?

Explanation: *It is necessary to ensure that all copies of personal data are tracked and managed in order to ensure their protection and deletion at the end of the data retention delay.*

☐ **No**

☐ **Yes**

…

17. Are the personal data stored in encrypted form?

Explanation: *As for the security issue, adequate measures should be adopted to safeguard the data stored and processed by the biometric system: personal information must always be stored in encrypted form. A key management framework must be defined to ensure that the decryption keys are only accessible on a need to know basis.*

Given the widespread use of public and private databases containing biometric information and the increasing interoperability of different systems using biometrics, the use of specific technologies or data formats that make interconnections of biometric databases and unchecked disclosures of data impossible should be preferred.

☐ **No**

☐ **Yes**

Explain

18. What are the physical security measures to protect the personal data?

Explanation: *Beside logical security mechanisms, the company should ensure physical security of the devices, so that they are not (physically) available for the attackers in order to extract personal data.*

☐ **No**
☐ **Yes**

Explain

19. Have you implemented anti spoofing measures?

Explanation: *To maintain the reliability of a biometric system and prevent identity fraud the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person. In respect of facial recognition, it may be critical to ensure that the face is a real one and not for example, a picture tied on an impostor's head.*

☐ **No**
☐ **Yes**

Explain

20. **Do you use biometric encryption?**

Explanation: *Biometric encryption is a technique using biometric characteristics as part of the encryption and decryption algorithm. In this case, an extract from biometric data is generally used as a key to encrypt an identifier needed for the service.*

This system has many advantages. With this system, there is no storage of the identifier or of the biometric data: only the result of the identifier encrypted with the biometrics is stored. Moreover, the personal data is revocable as it is possible to create another identifier that can be protected with biometric encryption as well. Finally, this system is more secure and easier to use to the person: it solves the problem to remember long and complex passwords.

However, the cryptographic problem to overcome is not easy because encryption and decryption are intolerant to any changes in the key, whereas biometric provides different pattern which may give rise to changes in the extracted key. The system must therefore be able to compute

the same key from slightly different biometric data, without increasing the False Acceptance Rate. The Working Party agrees that Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

☐ **No**

☐ **Yes**

Explain

1.3.3 **Access/disclosure conditions**

21. Which entity has access to the biometric data? Under which conditions?

Explanation: *The data controller has the obligation to implement appropriate technical and organizational measures to protect personal data against unauthorized disclosure or access. This means that the data controller should implement strong authentication mechanisms and a strict access policy that ensures that only duly authorized persons access the data for the performance of legitimate tasks. Data controllers can subcontract part of their activity to third parties (processors), provided that the processing is carried out on the behalf of the data controller. The processor should provide 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 (in writing or in another equivalent form) binding the processor to the controller and stipulating in particular that:*

- the processor shall act only on instructions from the controller,

- the processor 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.

Specific conditions apply to processors based outside the EU territory. For processors not based in a country that affords an adequate level of protection (see list here), the European Commission has published standard contractual clauses that could be used to regulate the transfers and further data processing activities (available here). In the case of controllers and processors belonging to the same multinational corporation, another possible solution could be the adoption of binding corporate rules approved by national data protection authorities.

Explain

22. Can data be transferred to third parties? Under which conditions?

Explanation: *Transfers of personal data to a third party that will not process the data on behalf of the data controller is in principle prohibited unless the transfer is compatible with the initial purpose of collection. Compatible means that the re-use of this information could have been expected by the data subject when sharing her data in the first place. This assessment shall be*

made on a case-by-case basis. Any other data sharing amounts to a new data processing activity that should have a specific legal basis.

Explain

23. Is data automatically deleted at the end of the retention delay?

***Explanation**: The data controller must ensure that all copies of the data is automatically deleted (including temporary copies created by the system, for example during the matching process). To make sure that all the versions of data are deleted; for example, all local copies of the videos and bodyprints must be deleted, new personal data aggregated from the initial collected data must be deleted, sending deletion request to third parties, to whom the personal data has been forwarded.*

☐ **No**
☐ **Yes**

Explain

24. What are the technical measures implemented to ensure accountability ?

***Explanation:** Access control logs and review reports should be maintained as the evidence that privacy requirements are properly implemented and complied with, including all information about any use of the data (with the identity of the agent), copy, transfer and deletion.*

…

***

Full Report generated – recommend to perform a second round of consultation of stakeholders.

Message to be displayed:

"We recommend that you perform a second round of consultation with the stakeholders. The goal of this second round is to provide information about the privacy risks that have been taken into account, the ones that have been discarded and the reason of the choices made. The mitigation measures taken should then be presented and explained. This includes the nature of the risk identified, the reasons why you identified this to be a risk, the interests at stake and the measures taken to reduce this risk." + provide a link to the consultation of stakeholders' questionnaire (for information)

Annex 5 - Final balancing - questionnaire phase 3

25. Does the biometric system translate a fair balance between individual's rights to privacy and data protection and the organization's interests? Summarize the main arguments.

Explanation: Such a question should be answered taking into account all aspects of the surveillance project. It is inserted in the final stage of the questionnaire in order for stakeholders to demonstrate their awareness regarding the impacts of the surveillance project on individual's privacy and data protection rights. Moreover, thoughtful efforts to answer this question can be used either in view of producing a privacy & data protection impact assessment, or as "accountability information".

Explain briefly

26. Have you checked with a lawyer or through consultation of the national data protection authority that the biometric system is, as designed, compliant with national legislation?

Explanation: This is a necessary verification before the deployment of the system in order to encure compliance with national legislation. National legislation may not only include data protection legislation, but also potential administrative law, labor law, videosurveillance law (in case of biometric cameras), or other relevant legislations…

Detail briefly

27. Have you completed, if applicable, the necessary notification/declaration/authorization request next to the national competent authorities?

Explanation: in several Member States, the processing of personal data, including biometric data, is subject to the prior notification to the national supervisory authority, and sometimes to its prior authorization.

Explain briefly (date of declaration or authorization request or reason why your system is exempted from such obligation).

Annex 6 – Governance: Guidelines to draft an internal privacy policy - Questionnaire: phase 3

1.1 Introduction

The purpose is to guide the user in order to define an internal privacy policy that includes policies and procedures regulating a given personal data processing activity. It takes the user throughout the different elements that an internal privacy policy should contain and provides explanations about the expected content of each section.

The concept of this questionnaire is based upon set criteria, detailed in the following seven categories:

1)Purpose of the processing

2)Data collection

3) Data accuracy

4) Data use and disclosure

5) Security

6) Rights of the data subjects

7) Governance structure

The following questionnaire is designed to provide a starting point to conduct an in-house privacy assessment and brief descriptions of key point notions are provided in each category.

1.2 Purpose of the processing

Each processing of personal data should have a clear, explicit and specified purpose. Processing of personal data refers to 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.

This means that the purpose should be defined before data are collected and, wherever relevant, data subjects should be informed of this purpose. The purpose should also be legitimate, in other words, the data processing activity should have a clear legal basis, i.e. the data processing activity should be based on one of the grounds listed by the 95/46/EC Directive (the Data Protection Directive)

The definition of the purpose is paramount as it will have an impact on several aspects of the data processing activities:

- Data collection: only data that are strictly necessary for the purpose of the processing must be collected. (see section 2)
- Data processing: the personal data processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. This obligation applies not only to the data collection phase but also throughout the processing. (see section 3)
- Further uses: Personal data should not be further processed in a way incompatible with the original purposes of collection. (Section 4).

It is thus paramount to clearly define the purpose of the data processing activity and ensure they adequately reflect the intentions of the data controller.

Questions	Type of answer	Import answer from Question n°
1. What is the purpose of the processing?	free	**1**
2. On which legal basis does the processing rely on?	List of choices: - Consent - Explicit consent (sensitive data) - Legitimate interests of the data controller - Contract - Performance of a legal obligation - Protection of the vital interests of the data subjects - Performance of a task carried out in the public interest	**8**

1.3 Data Collection

In respect of the data minimization principle (deriving from Article 6.1(b) and (c) of Directive 95/46/EC), the collection of personal information should be limited to what is directly relevant and necessary to accomplish a specified purpose and also, to be retained only for as long as is necessary to fulfil that purpose.

An organization needs to know what personal information it holds, how it is being used – and whether it really needs it at all. Understanding and documenting the types of personal information that an organization collects and where it is held are critically important. This will affect the type of consent the organization obtains from individuals and how the information is protected; and it will make it easier to assist individuals in exercising their access and correction rights. Every component of an accountable, compliant privacy management program begins with this assessment. Listing the different categories of data that will be processed is a necessary first step to further assess the adequacy of the information processed under the data minimisation and purpose specification principles, as well as to identify the data flows. As a good practice it is suggested that prior to setting up of a biometric information system, the controller maps out categories of data that may be included in the information system. The added value of this exercise it twofold. First, while performing this exercise the controller can evaluate risks associated with the collected personal data. Second, in response to identified risks that controller can take organisational and technical measures.

This means to be able to carry out an inventory of all personal data or categories of personal data being collected in order to be able to check at any time whether these data are still adequate, relevant and not excessive in view of the purposes of the processing. Specific

attention should be brought to the processing of sensitive data, whose processing is subject to stronger legal requirements.

This also means that data that are necessary for the purpose of the processing anymore should be deleted. It is thus of high importance to define personal data retention periods that are time-limited and appropriate to the purpose of the processing, in a way that personal data are stored no longer than is necessary for the purposes for which they are obtained and processed.

Questions	Type of answer	Import answer from Question n°
3. Which categories of data are necessary to achieve the purpose of the processing? Is there an inventory of personal data collected (categories and estimated number of data subjects)?	Free	**6-8**
4. Do the personal data reveal (directly or indirectly) racial or ethnic origin, political, philosophical or religious views, trade union membership, health information or information about an individual's sex life (sensitive data)?	free	**9**
5. Why is each category of personal data critical to achieve such purpose?	free	
6. Have you defined a retention period for each category of data? (Specify)	free	**14**
7. When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?		
8. How do you ensure that the data are destroyed/deleted/anonymised when the data retention period expires?	free	**15**

1.4 Data accuracy

The data controller must ensure that data are accurate throughout the data processing 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.

This means that adequate procedures are in place to correct inaccurate or incomplete information whenever the data controller gets knowledge of it either because of its own activities or because it is brought to its attention by the data subject. The data controller is also

under the obligation to communicate any update to be made to the third parties with whom the information has been shared.

Questions	Type of answer	Import answer from Question n°
1. Describe the procedure or technical means put in place to ensure data accuracy.	Free	**18**
2. Describe the procedure for people to update, amend or erase their personal information	free	
3. How do you inform third parties with whom the data have been shared of necessary updates?	Free	

1.5 Data use and disclosure

The data controller has the obligation to implement appropriate technical and organizational measures to protect personal data against unauthorized disclosure or access. This means that the data controller should implement a strict access policy that ensures that only duly authorized persons access the data for the performance of legitimate tasks. Data controllers can subcontract part of their activity to third parties (processors), provided that the processing is carried out on the behalf of the data controller. The processor should provide 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 (in writing or in another equivalent form) binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the processor 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.

Specific conditions apply to processors based outside the EU territory. For processors not based in a country that affords an adequate level of protection (see list here), the European Commission has published standard contractual clauses that could be used to regulate the transfers and further data processing activities (available here). In the case of controllers and processors belonging to the same multinational corporation, another possible solution could be the adoption of binding corporate rules approved by national data protection authorities.

Transfers of personal data to a third party that will not process the data on behalf of the data controller is in principle prohibited unless the transfer is compatible with the initial purpose of collection. Compatible means that the re-use of this information could have been expected by the data subject when sharing her data in the first place. This assessment shall be made on a case-by-case basis. Any other data sharing amounts to a new data processing activity that should have a specific legal basis.

It is thus recommended to keep track of all data transfers to third parties, be it controllers of processors. NIMITY, a Canadian think tank, has developed a tool directed to help data controllers keep track of this information.

Questions	Type of answer	Import answer from Question n°
1. Do you track whom you disclose which information to (subcontractors, commercial partners, etc.)?	Free	
2. Have you identified all third parties who have or could have legitimate access to personal data (if yes, have you determined their respective roles in the processing)?	free	**24**
3. Have you clearly defined in the instruments that regulate the transfer of/access to the data the obligations of the recipient?		
4. How do you ensure that third parties whom the data are disclosed to comply with their obligations in terms of personal data processing (due diligence)?	Free	
5. Do you transfer personal data outside EU borders?	Free	

1.6 Data and environment security

Appropriate technical and organisational measures, able to ensure an appropriate level of security in relation to the risks represented by the processing and the nature of the personal data to be protected, must be appropriately implemented. Such measures should prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and any other unlawful form of processing.

When there is a security breach, a complaint handling mechanism must be in place, involving people of relevant responsibility and ensuring that all needed persons in the organization are included in the resolution of the issue (e.g. representatives from technical, legal and corporate communications). A breach of security occurs where a stated organisational policy or legal requirement regarding information security has been violated. However, every incident which suggests that the confidentiality, integrity or availability of the information has been compromised can be considered a security incident. Every security breach will always be

initiated by a security incident which, only if confirmed, may become a breach. Therefore, an appropriate mechanism must be set in order to manage all the above mentioned situations.

Therefore, the responsibilities for internal and external reporting of the breach must be clear and reporting to privacy commissioners and notification of affected individuals may also be required.

Questions	**Type of answer**	**Import answer from Question n°**
1. Is there a records management system that assigns user accounts, access rights and security authorizations?	Free	
2. How do you protect the information against data breaches and misuse of personal information?		**24**
3. Which are the security safeguards that ensure the confidentiality of personal information? (e.g. encryption of digital records, all physical storage locked, etc.)		
4. Do your systems and applications provide audit trails of staff that have accessed electronic and personal records?		
5. What is the data retention and disposal plan?		
6. Is there a documented data breach response plan for management and staff to follow?		
7. Have you developed an Oversight and Review Plan (in order to review and adapt breach and incident management response protocols to implement best practices or recommendations and lessons learned from post incident reviews)?		

1.7 Rights of data subjects

Personal data must be processed fairly, meaning that the data processing activities should be transparent to the data subjects and comply with their reasonable expectations. The Data Protection Directive specifies which information should be provided to the data subjects, namely:

- the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;
- the purposes of the processing for which the personal data are intended;
- the period for which the personal data will be stored;

- the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
- in cases, where consent is required, provide a possibility to withdraw it;
- the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
- the recipients or categories of recipients of the personal data, and conditions under which data may be transferred to the recipients (e.g., access to a video may be provided upon an official request of a law enforcement agency);
- where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;
- any further information necessary to guarantee fair processing in respect of the data subject (e.g., the procedure for the repudiation, under which conditions re-enrolment procedure has to be repeated), having regard to the specific circumstances in which the personal data are collected;
- the level of security during all processing stages including transmission (e.g., over networks).

This information should be provided at the time of collection or when the data are not collected directly from the data subject at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

Data subjects also have a number of rights after the time of collection, directed to allow them to check which information is being processed about them and to ask for the correction of inaccurate information or its deletion. Finally, data subjects have a right to object to the processing activity under certain circumstances.

The data controller should therefore implement adequate procedures to ensure it can respond in a timely fashion to data subjects' requests. Some national laws set strict time limits to respond to these requests.

Questions	**Type of answer**	**Import answer from Question n°**
1. When and how are data subjects informed of the processing activity and of their rights to access, rectification, deletion and objection?		
2. Is the information provided in a clear language, understandable by a person who is not familiar with information technologies or the Internet?		
3. Is there evidence that the information notice was provided? (notice or document signed, other):		
4. Which are the internal procedures put in place to deal with requests of data subjects		

for access, rectification, deletion, objection? (specify)		
5. What is the maximum time response?		

1.8 Governance structure

An accountable organization is expected to ensure and demonstrate compliance with the legal framework. Thus, accountability entails no more than an assumption and acknowledgement of responsibility and an obligation to demonstrate compliance upon request to the competent supervisory authority.

From a legal perspective, accountability is therefore concerned with the design and implementation of policies, procedures and practices that will aim at ensuring and demonstrating legal compliance. This means to designate a person within the organization who will be responsible to implement and monitor the internal privacy policy, inform and train persons with access to personal data, to install assurance mechanisms (internal or external audits) and report to the management about the privacy management program.

It is thus first recommended to designate a person within the organization responsible to monitor their implementation, such as a Data Protection Officer (DPO).

The DPO, or equivalent, should be responsible in particular for independently ensuring the internal application of the national data protection legislation, for keeping a register of personal data processing activities performed by the organization, and for ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations. Also, a DPO has an information and raising awareness function (staff information notes, training sessions, privacy statements), an advisory function (recommendations for the practical improvement of data protection and consulting the organization and the staff committee, as well as any individual), a monitoring of compliance function and a function of handling queries or complaints. The DPO must carry out his/her duties directly alongside the data controller with organizational and decisional freedom and without any conflict of interests. He/she must be provided with adequate human and financial resources and to have access to information and to offices and data-processing installations.

It is then recommended to define assurance mechanisms. Assurance mechanisms are also related to accountability and in particular, internal audit and assurance programs to monitor compliance with privacy policies are crucial within an organization. An effective reporting program defines clearly its reporting structure (in terms of reporting on its overall compliance activities), as well as employee reporting structures in the event of a complaint or a potential breach and tests and reports on the results of its internal reporting structures, while documenting all of its reporting structures. Reporting mechanisms need to be established and reflected in the organization's program controls. The organization needs to establish internal reporting mechanisms to ensure that the right people know how the privacy management program is structured and whether it is functioning as expected.

Also, conducting risk assessments, at least on an annual basis, is an important part of any privacy management program to ensure that organizations are in compliance with applicable legislation. Organizations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk

assessments. Finally, it is of high importance for organization to develop an oversight and review plan, in order to keep its privacy management program up to date.

Finally, it is recommended to communicate privacy policies to their recipients to ensure they are aware of and understand their content. The way how privacy policies are communicated is key to ensure they are implemented efficiently. Also, up-to-date training and education requirements for all employees, tailored to specific needs, are key to compliance. In order for a privacy management program to be effective, employees must be actively engaged in privacy protection.

1.8.1 **The Data Protection Officer**

Questions	**Type of answer**	**Import answer from Question n°**
1. Who is responsible for the implementation and management of the internal privacy policy?		
2. Who is responsible for program controls and who endorses them?		
3. Are the roles and responsibilities of the actors involved in the processing clearly defined?		
4. Is the scope of DPO's competences well defined and which human, technical and financial resources have you allocated to support the DPO's activities?		
5. Is the DPO systematically involved in exchanges/contacts with Data Protection Authorities?		
6. Is the DPO systematically involved in exchanges/contacts with Data Protection Authorities?		

1.8.2 **Assurance mechanisms**

Questions	**Type of answer**	**Import answer from Question n°**
1. Who is responsible for program controls and who endorses them?		
2. Do you have a clearly defined internal reporting structure?		
3. Have you set up a documentation mechanism		

for all reporting structures?		
4. How do you ensure that privacy risks are assessed on a regular basis and at least whenever a new product/service/system is being developed?		
5. How often do you perform internal or external compliance audits and how are correction measures implemented? (If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the project design?)		
6. How do you ensure that privacy risks are assessed on a regular basis and at least whenever a new product/service/system is being developed?		

1.8.3 **Communication of the privacy policy**

Questions	**Type of answer**	**Import answer from Question n°**
1. How do you intend to communicate the privacy policy to staff?		
2. Do you train your staff and subcontractors or partners about internal privacy policies?		

***