PrivAcy pReserving Infrastructure for Surveillance

Deliverable D2.3
Guidelines for Use Cases for SALT Frameworks

Project: PARIS
Project Number: SEC-312504
Deliverable: D2.3
Title: Contexts and concepts for SALT Frameworks
Version: v1.0
Date: 13/06/2014
Confidentiality: Public

Editors: François Thoreau (CRIDS-UNamur)
Claire Gayrel (CRIDS-UNamur)
Francisco Jaime (UMA)

Contributors: Claire Gayrel
François Thoreau (CRIDS-UNamur)
Fanny Coudert (ICRI-KU Leuven-iMinds)
Zhendong Ma, Bernhard Strobl (AIT)
Daniel Le Métayer, Denis Butin (INRIA)
Antonio Kung, Christophe Jouvray (Trialog)

Part of the Seventh Framework Programme
Funded by the EC - DG INFSO

Table of Contents

EXECUTIVE SUMMARY 4
LIST OF FIGURES 5
LIST OF TABLES 5
ABBREVIATIONS AND DEFINITION 6
1 INTRODUCTION 8
1.1 Deliverable objective and scope 8
1.2 A domain approach 9
1.3 Inputs and outputs of guidelines 10
2 CONCEPTS OF SALT FRAMEWORKS FOR USERS 12
2.1 A questionnaire-based approach 12
2.2 A compagnon to the 3 stage-process 14
2.3 Step-by-step procedure and user guidelines 16
3 GUIDELINES FOR USERS BY DOMAIN 18
3.1 For Socio-contextual and ethical dimensions 18
3.1.1 User roles 18
3.1.2 Purpose and limits 19
3.1.3 Methodological guidelines 20
3.1.3.1 Inclusiveness of the process 20
3.1.3.2 Dynamic use 20
3.1.3.3 A closing procedure 21
3.1.3.4 Situating the system 21
3.1.3.5 Principle of delegation 21
3.2 For the legal dimension 22
3.2.1 Main goals of the SALegal Questionnaire 22
3.2.1.1 Integrate both high privacy and data protection standards 22
3.2.1.2 Turn the principle of proportionality from theory to practice 22
3.2.1.3 What can SALT users expect from the SALegal Guidelines 22
3.2.2 Step-by step methodology 23
3.2.2.1 Stage 1 — “Opportunity” 23
3.2.2.2 Intermediary stage: checking national legal requirements 25
3.2.2.3 Stage 2: “Design” 25
3.2.2.4 Stage 3: Final balancing 27
3.2.3 Out of scope of the SALT framework: data protection and other compliance check 28
3.2.4 Example of use cases of the SALT framework in relation to biometric systems 30
3.2.4.1 Use case n°1: installation of a biometric system to control access to school restaurant 30
3.2.4.2 Use case n°2: installation of a biometric system to control working time of employees 30
3.2.4.3 Use case n°3: installation of a biometric system to control access to an amusement park 31
3.3 For Technical dimensions 32
3.3.1 User roles 32
3.3.2 Objectives of guidelines 32
3.3.3 Guideline for SALT building process 33
3.3.4 Guideline for SALT use process 33

3.3.5 A first example: Biometrics guidelines 34
3.3.6 A second example: Video-surveillance technical guidelines 35
3.4 Accountability 36
3.4.1 Goals of accountability mechanisms 36
3.4.1.1 Answerability 36
3.4.1.2 Verifiability 37
3.4.2 What can SALT users expect from the guidelines related to accountability 37
3.4.2.1 SALT experts 37
3.4.2.2 Decision makers (surveillance system owners) 38
3.4.2.3 System designers 38
3.4.2.4 System operators 39
3.4.3 Accountability mechanisms in Ethical, Legal and Technical viewpoints 39
3.4.3.1 Ethical viewpoint 39
3.4.3.2 Legal viewpoint 41
3.4.4 Technical viewpoint 43
3.4.5 Accountability mechanisms in the SALT process 44
3.4.5.1 Step One: Intention 45
3.4.5.2 Step One bis: Checking national requirements 45
3.4.5.3 Step Two: Integration of considerations 46
3.4.5.4 Step Three: overall assessment and system lifecycle 47
4 CONCLUSIONS 48

DOCUMENT HISTORY

Version	Status	Date
V0.1	Liminal draft	01/05/2014
V0.2	Provide content to all Sections	9/05/2014
V0.3	Revision of the structure of the document	12/05/2014
V0.4	Integration of all contributions	03/06/2014
V0.5	Preparation for internal review	11/06/2014
V0.6	Integration of reviewer's comments	13/06/2014
V1.0	Finalization of the document	13/06/2014

Approval		
	Name	**Date**
Prepared	François Thoreau	11/06/2014
Reviewed	Antonio Kung	12/06/2014
Authorised	Antonio Kung	13/06/2014

Circulation	
Recipient	**Date of submission**
Project partners	13/06/2014
European Commission	13/06/2014

Executive Summary

D2.3. relies upon key findings from D2.1. and D2.2 and targets SALT users, i.e. the people in charge of applying the SALT frameworks. It provides tentative guidelines for future users of SALT framework. Mostly, it addresses 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 which aims to define and make operative the concepts of SALT framework.

List of Figures

Figure 1 Integrating dimensions for a domain approach 10
Figure 2 SALT framework, SALT reference and SALT process 14
Figure 3 Three stage process for SALT Framework 15
Figure 4 Overview of the use of the SALegalT framework in relation to biometric systems with the examples of France an Belgium 29
Figure 5 SALT knowledge at different steps of the development cycle 34
Figure 6 Guideline for SALT use process.....34

List of Tables

Table 1 User roles for technical dimensions 32

Abbreviations and definition

Abbreviation	Definition
1D	One-Dimensional
2D	Two Dimensions
3D	Three Dimensions
APEC	Asia Pacific Economic Cooperation
ARPT	Active Reader Passive Tag
Article 29 WP	Article 29 Data Protection Working Party
BAP	Battery Assisted Passive
CCTV	Closed Circuit Television
CIA	Confidentiality, Integrity and Availability
CNIL	Commission Nationale Informatique et Libertés (FR)
COE108	Council of Europe Convention 108
CPU	Central Processing Unit
DNA	Deoxyribonucleic Acid
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
GPS	Global Positioning System
IA	Impact Assessment
ICT	Information and Communication Technologies
ID	Identity
IdM	Identity Management system
IM	Instant Messaging
IP	Internet Protocol
JO	Journal Officiel (FR)
LBS	Location-Based Services
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
PRAT	Passive Reader Active Tag
RFID	Radio Frequency Identification
RTP	Real Time Transport
SALT	Social, ethicAl, Legal, Technical
UAV	Unmanned Aerial Vehicle
US	United States
USA	United States of America
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity
WP	Working Party (e.g. OECD)

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 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.

The present document D2.3. relies upon key findings from D2.1. and D2.2 and targets SALT users, i.e. the people in charge of applying the SALT frameworks. It provides tentative guidelines for future users of SALT framework. Mostly, it addresses 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 which aims to define and make operative the concepts of SALT framework.

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", assuming that the most relevant entry point to SALT framework depends upon the user's desired level of expertise. Then the introduction makes a point about the status of current guidelines in this deliverable, what it targets and what it aims for.

The section 2, “Concepts of SALT frameworks for users” introduces the main concepts used in SALT framework in an easy and understandable way, so that SALT users may easily apprehend what SALT framework are about, what they deal with and what they encompass. It start 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 stage of development of a surveillance system into public space: 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 then 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. 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. Third, it deals with the technical dimensions and identify the relevant technical users and provides step-by-step guidelines which will take him/her through the development process. Lastly, we examine the accountability dimension. This dimension cross-cut many aspects of both the socio-contexual and ethical, legal and technical dimensions. Since it rests at the intersection of both three sections, it appears useful to wrap up SALT procedures and to fully complete SALT Framework so as to make them truly comprehensive.

1.2 A domain approach

SALT frameworks are interdisciplinary in scope. They encompass a wide variety of perspectives and put experts from different disciplines together, i.e. 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 SALT 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 always easy for experts from different disciplines to come together and design a unique SALT framework. To give but on 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 represent in a digital manner the legal requirements.

However, no matter how difficult it is, interdisciplinarity allows for integrating various viewpoints and dimensions. In this respect, it is very challenging and this challenge we took 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. That is 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, still he will 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, it is precisely the circle described in Figure 1, which rests at the middle of the four mentioned domains. This means that SALT framework 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.

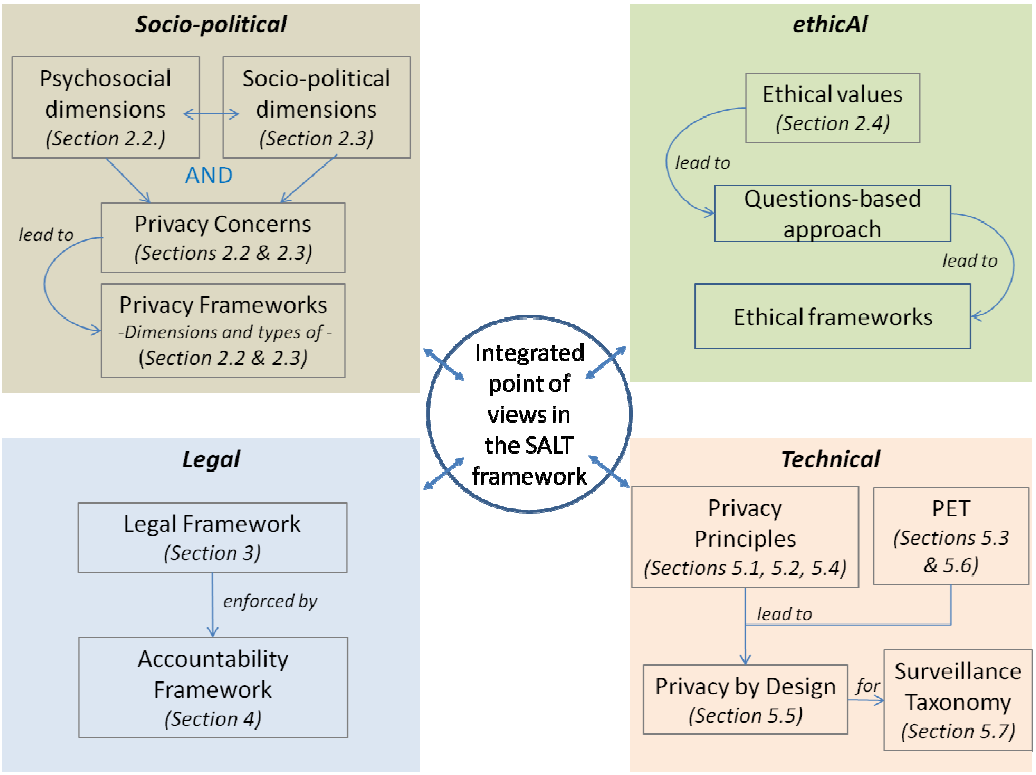

Figure 1 Integrating dimensions for a domain approach

1.3 Inputs and outputs of guidelines

Guidelines are made for SALT users and SALT owners mainly, but this depends on each kind of targeted domain. In section 3, we detail which kind of users are targeted by which kind of guideline, depending on the specifics of each of those domains.

The guidelines are methodological tools which aim at taking the SALT user through the whole process of designing surveillance system in public spaces. They facilitate the introduction to SALT concepts and vocabulary, and they render explicit how to use the SALT reference 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 are both limited and very interesting. They are limited because SALT cannot achieve mechanical compliance, by determining socio-contextual and ethical, legal, technical and accountability “parameters” too rigidly. Which means that the responsibility of the output of the system rests with the users, who cannot stay passive and has 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 from taking into considerations other fields of expertise or other domains than the one he is accustomed to. For instance, the SALT reference 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 is cumulative and expect 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 very rewarding system because it facilitates users’ inputs.

The consequence of all this is that the SALT representation goes away from strict legal compliance as initially considered, but crafts something which causes a reflection on socio-contextual and ethical, legal, technical and accountability issues. Compliance thus rests with the process instead of 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 raise by itself. For that, it takes close consideration from 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 grant him with added value through the amount of expertise made available.

This deliverable is intended to the user to learn how to use SALT frameworks, in order for the user 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 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 **S**ocio-contextual and ethic**A**l, **L**egal, and **T**echnological.

In addition, 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 customise 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 stage process, that is the various normal stages of development of a surveillance system in public space. 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, 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 is sequential and can take the SALT user through the process of conceiving, designing and implementing a SALT system, i.e. a system of surveillance in public space. 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 compagnon to the 3 stage-process

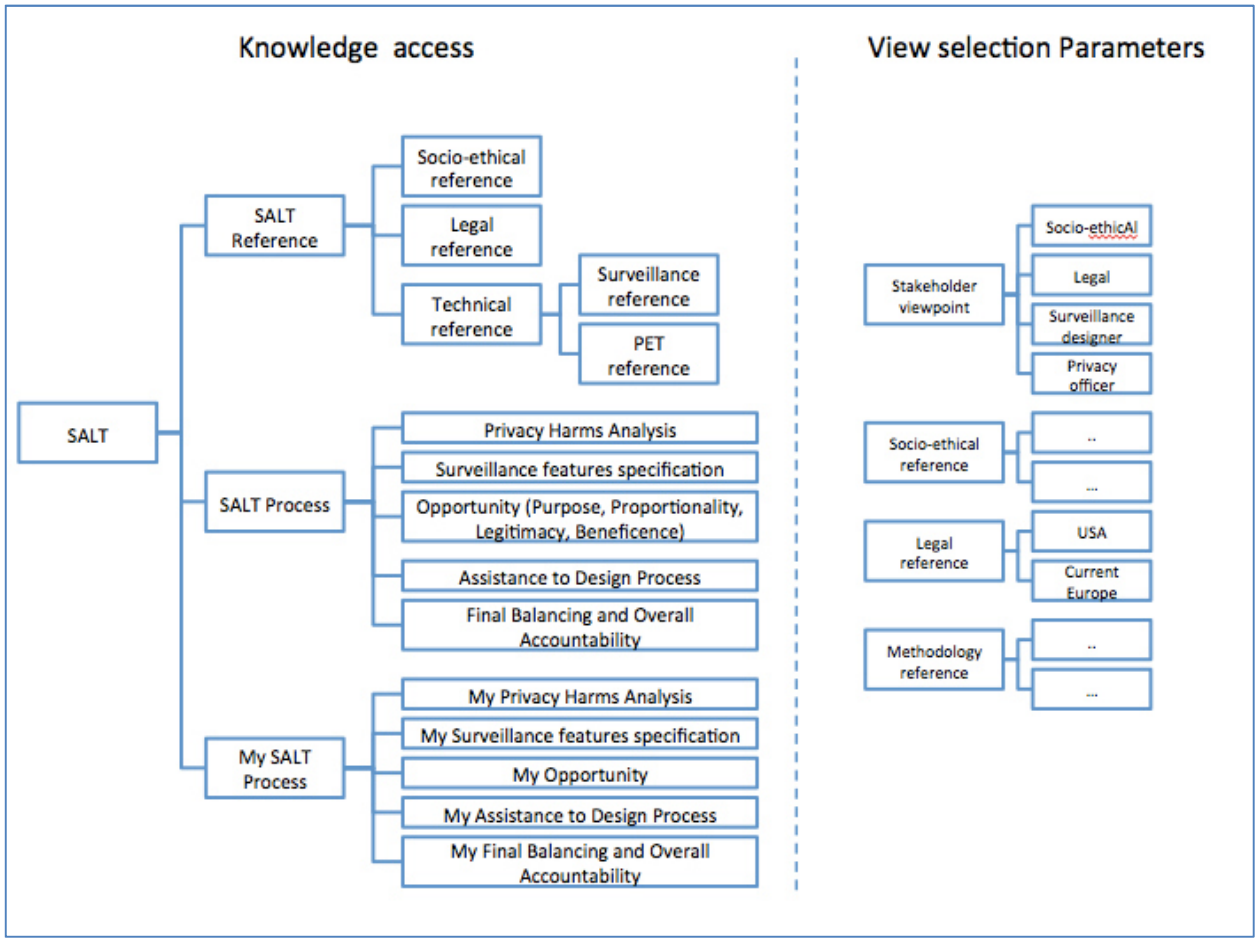

Figure 2 SALT framework, SALT reference and SALT process

This picture shows the overall SALT framework as it includes a body of knowledge called SALT reference, and a SALT process. In D2.3., we offer guidelines which concern more particularly the SALT Process as described in the left-hand column. Below we describe what we call a “three-stage process” which fits within this overall SALT framework, and which uses SALT reference to perform.

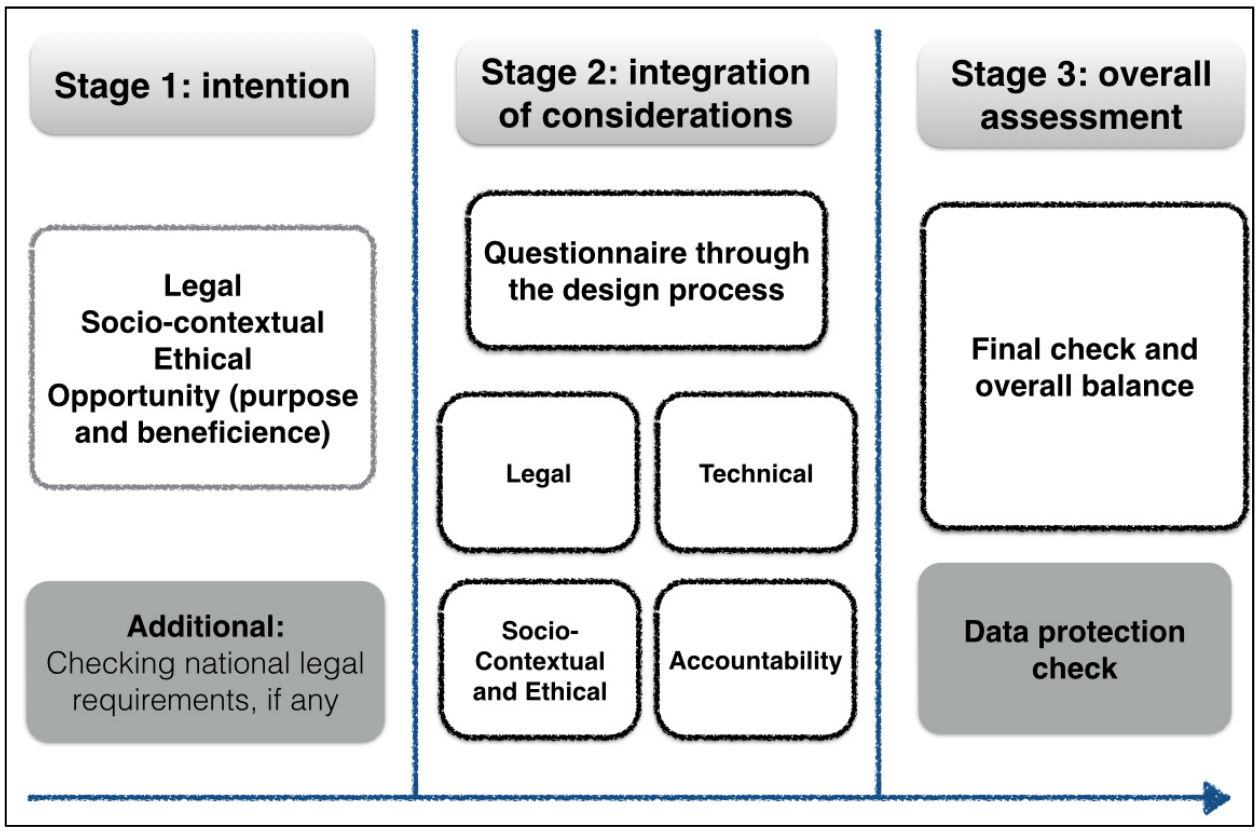

Figure 3 Three stage process for SALT Framework

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 in public space 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 video 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 assesses different questionnaires throughout the design process, i.e. legal, socio-contextual and ethical, technical, and as for the accountability. All the questionnaires are knowledge-based and represented as SALT instances in the SALT framework.

Finally, when all the system is designed and that answers to all the questionnaires has 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 and ethical and legal proportionality and opportunity.

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 are 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.

2.3 Step-by-step procedure and user guidelines

In section 3 we will offer guidance for SALT users with respect to the use of SALT frameworks. We suggest provisional guidelines to follow for using the SALT frameworks. Here, guidelines are methodological tools which help apprehend and frame the SALT frameworks. That is their purpose is to facilitate user's experience of SALT frameworks and to combine adequately the different sort of expertise that are present in the SALT.

First, it will facilitate SALT users' experience by taking them through the process of defining and developing a system of surveillance in public spaces. It will accompany them stage by stage, according to the picture mentioned above (2.2.) while providing grounds to revisit further evolutions of the project. It is like a map which will allow user to find their ways into the manifold and complex dimensions which the SALT encompasses, i.e. legal, socio-contextual and ethical, technical and accountability.

Second, this is needed precisely because the SALT is so interdisciplinary in scope. It is perfectly understandable that en engineer doesn't have the prerequisite to grasp ethical issues, the same way an ethicist does not necessarily understand technical aspects. This is why those guidelines are important for the user, because he/she will be able, step after step, to go through the whole process while being guided. Useful insights into those different dimensions will be provided to him/her so as potentially get to address all of them.

It is important to mention that these guidelines are still at a conceptual level. It is planned in the description of work that a second updated version of the guidelines will be released to take into account the actual evolution of the SALT framework and of the SALT knowledge repository.

Furthermore, even yet, the guidelines are not meant to be written once and for all. As a matter of fact, they are supposed to evolve over time according to SALT users feedbacks. As methodological tools which help apprehend and frame the SALT frameworks, they will need to be tailored according to further evolutions of the project.

3 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.

3.1 For Socio-contextual and ethical dimensions

3.1.1 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 had 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.

3.1.2 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 into mind so as not to expect out of the SALT framework something which 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. Usually, the socio-contextual and ethical dimensions rely on existing references so as not to reinvent solutions which 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 D2.2. 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 to say 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 offers 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.

3.1.3 Methodological guidelines

3.1.3.1 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, we strongly encourage the use of SALT framework in combination with other participatory tools (consensus conferences, citizen jury, focus group, Delphi methodology) so as to widely engage stakeholders and enhance the views on socio-contextual and ethical dimensions.

3.1.3.2 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 which are made in between. This fits with the three stage process described in section 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 security system in a public place.

In social science 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, "downstream" 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 socio-contextual and ethical questionnaire crafted in D2.2. is 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.

3.1.3.3 A closing procedure

As stated in 3.1.3.1., the process should be as inclusive as possible, for 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 nor 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.).

3.1.3.4 Situating the system

Socio-contextual and ethical dimensions always depend of the specificities of the current system which 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 such as the one we extensively presented in D2.1. and D2.2. There is no simple recipe.

3.1.3.5 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 an history, 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.

3.2 For the legal dimension

Preliminary remark

At this stage of the project, the following draft guidelines are provided in relation to biometric systems only. Further guidelines need to be elaborated in relation to videosurveillance systems. The present guidelines are widely elaborated upon D.2.2 findings.

3.2.1 Main goals of the SALegal Questionnaire

3.2.1.1 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.

3.2.1.2 Turn the principle of proportionality from theory to practice

A major goal of the SALegalT 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. 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.

3.2.1.3 What can SALT users expect from the SALegal Guidelines

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.

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.

3.2.2 Step-by step methodology

3.2.2.1 Stage 1 — "Opportunity"

Goal: This first stage focus 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.

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

Format: questionnaire with associated explanations/recommendations.

Example of question in relation to the "Legitimacy" of the project

On which legal ground you will be relying on as providing a legitimate basis for the implementation of the biometric system?

The European Directive requires that personal data may be processed only under a limited and exhaustive list of circumstances that delineate the legitimate grounds for the processing of personal data.[1]*For three of these grounds (which are the more likely to concern stakeholders using the SALT framework), subquestions are drafted in order to help the relevant stakeholders to check whether or not the envisaged legitimate ground is likely to be valid.*

a. Consent of the data subject?

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."[2] *If the notion of 'indication' is wide (insofar as it can take*

[1] The draft questionnaire will take into account only three of the grounds. Are not considered here the processing of personal data for "compliance with a legal obligation" (Art. 7 (c)); processing "necessary to protect the vital interest of the data subject" (Art. 7 (d)) and processing "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" (Art. 7 (e)).

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

different forms), it seems to imply a need for action. In order to be 'freely given', the data subject must be able to exercise a real choice, and the refusal to provide consent should not entail negative consequences. 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. To be valid, the consent must also be specific to a processing which has itself a specific purpose. Finally, there must always be information before there can be consent. 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 is validly grounded.

If yes, check the following conditions:

- **There is no significant imbalance between the position of the data subject and the controller.[3]**

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.[4]

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

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.[5]**

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**

Et cetera…

Expected effects: Following these three sets of questions, the organization at the initiative of the implementation of a surveillance system should start to have a primary view over the

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

[4] Recital 34 of the proposal of Regulation

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

legitimacy and necessity to recourse or not to a biometric system for the stated purposes/objectives.

For instance, in case of insufficiently robust legitimate ground (e.g. Weak consent for example), the whole project of biometric system should be put in question. 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 preliminary assessment should not lead to any conclusions regarding the proportionality of the system, which requires consideration of all functioning aspects of the system.

If the results of such assessment prove to be sufficiently robust, deciders should turn to national legal requirements to see how the technology is (or not) regulated.

3.2.2.2 Intermediary stage: checking national legal requirements

Interested stakeholders: lawyers

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.

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

Format: general legal information regarding national requirements in relation to a specific technology, if any

3.2.2.3 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 Authorithies, the so-called Working Party 29.

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

Format: questionnaire with associated explanations/recommendations.

Example of questions in relation to the "storage" of data:

1. Are the raw data stored as biometric templates?

Biometric data should be stored as biometric templates whenever that is possible. Template should be extracted in a way that is specific to that biometric system and not used by controllers of similar systems in order to make sure that a person can only be identified in those biometric systems that have a legal basis for this operation.

What is the size of the template?

The size of the template should be wide enough to manage security (avoiding overlaps between different biometric data), but should not be too large so as to avoid the risks of biometric data reconstruction

Is it possible to regenerate the raw biometric data from the template?

The generation of the template should be a one way process.

2. Where is stored the data obtained during the enrolment?

Are they stored locally where the enrolment took place?
Are they stored on a device carried by the individual?
Are they stored in a centralized database?

Whenever it is permitted to process biometric data, it is preferred to avoid the centralized storage of the personal biometric information.

Especially for verification, the Working Party considers advisable that biometric systems are based on the reading of biometric data stored as encrypted templates on media that are held exclusively by the relevant data subjects (e.g. smart cards or similar devices). Their biometric features can be compared with the template(s) 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 data subject should be stored in such devices.

However, for specific purposes and in presence of objective needs centralised database containing biometric information and/or templates can be considered admissible. The biometric system used and the security measures chosen should limit the mentioned risks and make sure that the re-use of the biometric data in question for further purposes is impossible or at least traceable. Mechanisms based on cryptographic technologies, in order to prevent the unauthorised reading, copying, modification or removal of biometric data should be used.

When the biometric data are stored on a device that the data subject physically controls, a specific encryption key for the reader devices should be used as an effective safeguard to protect these data from unauthorised access. Furthermore such decentralised systems provide for a better protection of the biometric data by design as the data subject stays in physical control of his biometric data and there is no single point that can be targeted or exploited. The Working Party also stresses out that the idea of centralised database covers a wide range of technical implementations from the storage within the reader to a network hosted database.

Expected effects: 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.

3.2.2.4 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

Example of question:

1. **Does the surveillance system translate a fair balance between individual's rights to privacy and data protection and the organization's interests? Summarize the main arguments.**

Such a question should be answered taking into account all aspects of the surveillance project. 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. 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".

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".

3.2.3 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.

In blue: steps covered by the SALT questionnaire
In grey: steps not entering within the scope of the SALT questionnaire

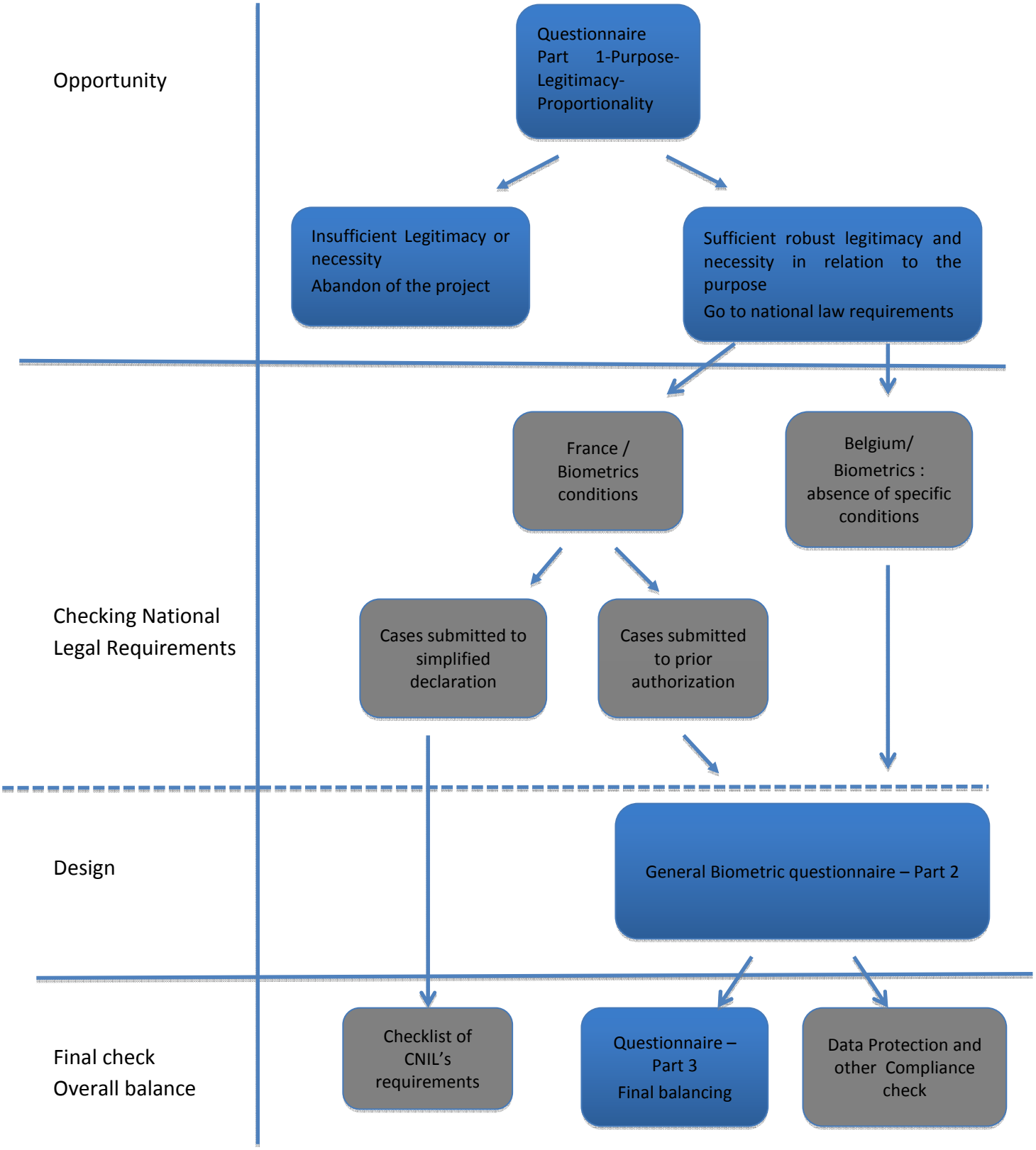

Figure 4 Overview of the use of the SALegalT framework in relation to biometric systems with the examples of France an Belgium

3.2.4 Example of use cases of the SALT framework in relation to biometric systems

3.2.4.1 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 assess 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.

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 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.

3.2.4.2 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).

At first, they imagined to include a specific clause in the employment contracts specifying that employees shall accept enrolment in the biometric system. They therefore turned to legitimate ground b) "Performance of a contract to which the data subject is party". However, as explained by the SALT questionnaire, this legitimate ground will apply in general only when pure biometric services are provided to the data subject. Since this is not the case of employment contracts, legitimate ground b) cannot be validly invoked. Second, the lawyers envisage to obtain the written consent of their employees for the enrollment into the system.

Again, they find out that employees' consent is not an adequate legitimate ground following the explanation provided under a) in this specific case because of the significant imbalance between the employees and their employer. They finally turn to the legitimate ground c) invoking the legitimate interests of the employer to control the working time of his employees. Although, the control of employees is a sensitive issue, the employers' lawyers believe their interests are legitimate and prevail over the interests of their employees.

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.

3.2.4.3 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 envisages to invoke his legitimate financial interests to justify the recourse to a biometric system (legitimate ground c) of Q.2.) However, considering the explanation provided by the SALT framework according to which "*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",* the owner decides not to rely on such ground. Indeed, although his financial interests might be considered as legitimate, such a justification does not appear sufficiently robust to assert that they prevail over individuals' rights. Instead, the owner, decides to rely on the consent of his subscriber 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.

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.

3.3 For Technical dimensions

This subsection outlines the high level requirements and format of guidelines for use cases of SALT conceptual framework. We leverage the use cases we had in D5.1 for video surveillance system and D6.1 for biometric system to provide a preliminary "look and feel" to develop the guideline for technical dimensions. The guidelines will be refined in accordance with the progress in the technical use case development. An updated version will be appeared in D2.4.

3.3.1 User roles

The guideline for the technical dimension is envisioned to streamline activities and processes concerning the user interaction with the SALT conceptual framework. In other words, the guideline should be a set of useful instructions on how to interact with the SALT framework.

From a technical perspective, the following general roles can be assumed by a user of the SALT framework.

Roles	Description
SALT expert	They use the tool to create/update new instances/reference. They need to provide complete and accurate content.
System designer	(1) Systems owners who are responsible for the definition of surveillance and high level system requirements. (2) System designers who are responsible for the realization of requirements in technical solutions.
System Operator	People who operate and maintain the system after its provision. They will make operational decisions on a day-to-day basis.

Table 1 User roles for technical dimensions

It is likely that an individual will have multiple roles. For example, in the PARIS project, one can assume the role of SALT expert during the SALT conceptual development, as well as the role of system designer during the demonstration phase.

3.3.2 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.

3.3.3 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.

3.3.4 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.

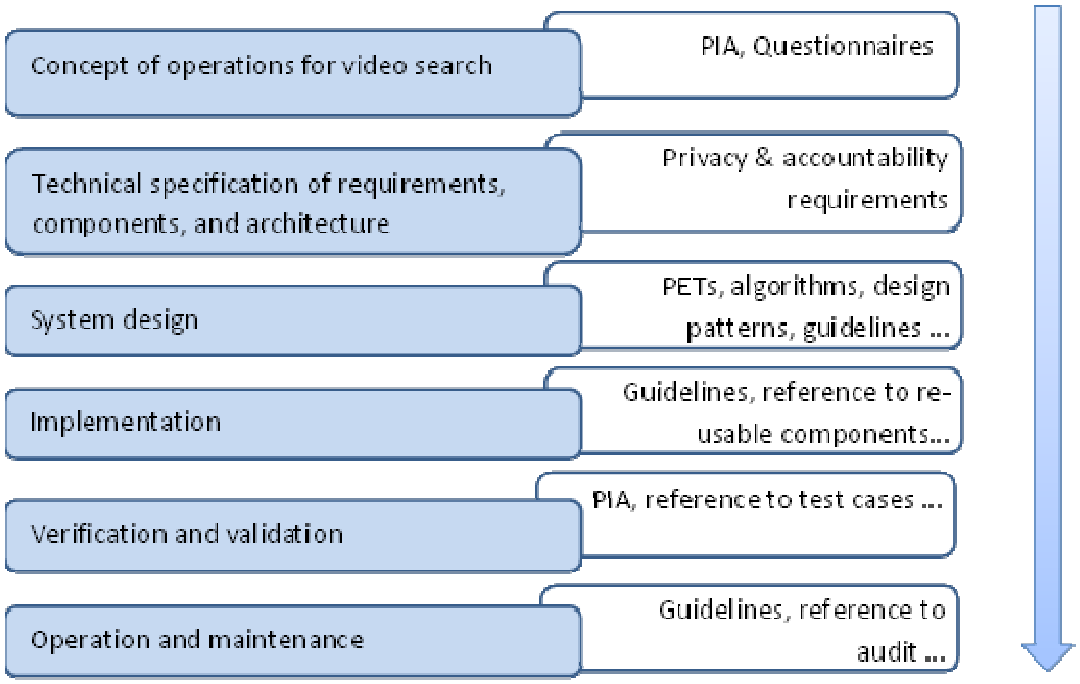

Figure 5 SALT knowledge at different steps of the development cycle

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.

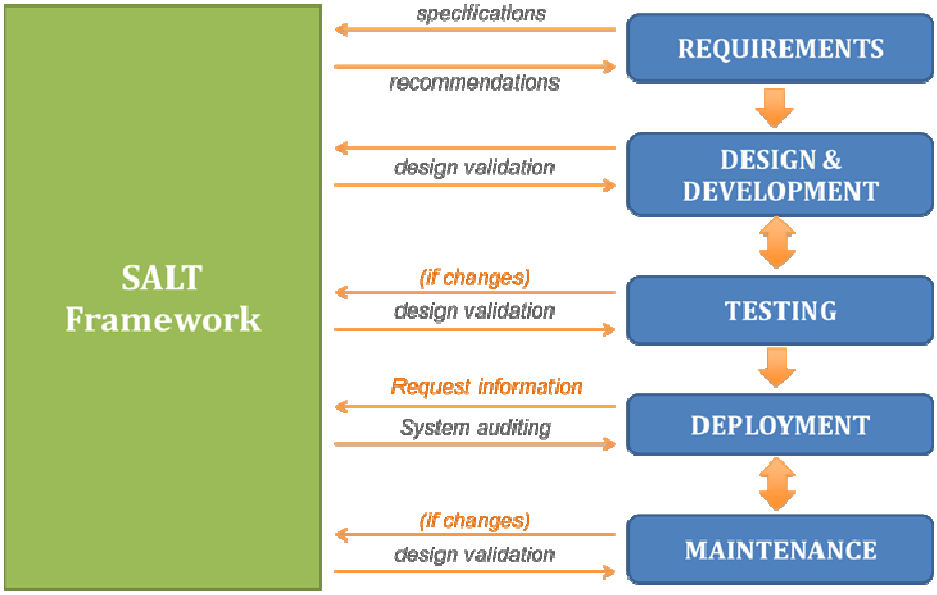

Figure 6 Guideline for SALT use process

3.3.5 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.

3.3.6 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.

3.4 Accountability

Accountability in the SALT Framework

The SALT framework incorporates a dedicated section to accountability mechanisms in each of the three viewpoints (ethical, legal, technical).

The goals of accountability mechanisms are twofold: (1) to ease answerability and (2) to increase verifiability. In order to reach these goals, several mechanisms are presented to the SALT user. These accountability mechanisms will vary depending on the viewpoint of the SALT framework involved and on the design phase in which the SALT Framework user is interested in: before design phase ("intention"), during system design (stage 2 "integration of considerations" and 3 "overall check"), during system lifecycle.

This section presents the goals of accountability mechanisms, what each SALT user can expect from the information on accountability provided in the SALT framework and an explanation of how accountability aspects are approached from each of SALT viewpoints and at each stage of the SALT process. The examples provided are not use case specific. They rather intend to give a general idea of what the final questionnaires will look like.

3.4.1 Goals of accountability mechanisms

3.4.1.1 Answerability

Answerability is "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".[6]

In that context accountability is about:

- engaging with, and being responsive to stakeholders;
- talking into consideration their needs and views in decision-making;
- providing an explanation as to why they were or were not taken on board[7].

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

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

The ultimate goal is to generate ownership of decisions and projects by all involved stakeholders and to enhance the sustainability of activities of the accountor[8].

Accountability mechanisms give transparency by actively engaging the accountor in a dialogue with the relevant stakeholders. 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.

3.4.1.2 Verifiability

Verifiability means that the actions and decisions of the surveillance system owners and operators are registered and can be checked internally or by an independent third party.

Accountability mechanisms are concerned with 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. Accountability mechanisms should serve to demonstrate the entity abides by the applicable legal framework, contractual agreements, etc.

As a way of example, technology will support this goal by providing tools to define data handling policies, specify the design of processing evidence in execution traces called logs and implement automatic a posteriori compliance checking mechanisms between policies and logs. In that sense, it offers three capabilities: (a) Validation (checking log compliance with respect to policies); (b) Attribution (allocating responsibilities); (c) provision of evidence.

3.4.2 What can SALT users expect from the guidelines related to accountability

3.4.2.1 SALT experts

SALT experts facilitate accountability by providing the future SALT users with detailed information on building accountable systems. To be useful in practice, this information must be as specific as possible and the best way to achieve this is to distinguish between the largest possible number of configurations.

An important parameter is the jurisdiction, since national laws may be relevant in addition to EU regulations or directives. Whenever the applicable legal framework provides for specific obligations in terms of accountability (e.g. consultation processes, reporting mechanisms, organizational and technical processes), reference to these texts will be made.

[8] The accountor is the entity who has committed or is obliged to give an account of its practices. In the context of the SALT framework, the accountor will most likely be the surveillance system owners, in its quality of data controller.

Accountability mechanisms can relate to internal and external policies, procedures and practices (data processing activities). The SALT framework should provide recommendations to guide surveillance system owners and system designers for their implementation.

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.

3.4.2.2 Decision makers (surveillance system owners)

Decision makers, i.e. the entities responsible for the design and implementation of a new surveillance system, have a duty to ensure the acceptability and legitimacy of the system to be implemented. The SALT framework will guide them in managing the consultation process with the relevant stakeholders (answerability) and in incorporating the most adequate mechanisms to ensure the verifiability of their practices.

3.4.2.3 System designers

System designers have the most critical role in enabling verifiability, because their decisions impact the kind of evidence that is available to demonstrate compliance. Designers are guided by the SALT Framework for integrating mechanisms of accountability that will ensure the verifiability of personal data processing activities.

Since the guidance provided by the framework depends on the configuration of the system, it is important that the initial input (the answers to the questionnaire) reflect both original intent and final execution. System designers must ask themselves the following questions to get the best results in terms of accountability:

- Have all privacy concerns, data categories involved in processing and purposes of processing been identified exhaustively?

- Has the questionnaire been filled out to mirror the aforementioned items as precisely as possible?

- Has all guidance provided by the SALT Framework been not only taken into account, but also checked for completeness?

- In particular, was both EU law and national law taken into account? In case of mismatch, the most restrictive text applies.

- Does the system feature novel privacy threats that were not taken into account or covered by the questionnaire?

- If so, what measures can be taken into account to enable accountability for these aspects also, taking into account the principle of accountability as a demonstration of compliance with both the legal framework and other commitments?

3.4.2.4 System operators

System operators must be provided with adequate and comprehensive documentation. In particular, it is not enough for a system to integrate accountability features if they are not put to use. As stewards of the system, system operators must be familiar especially with technical aspects of accountability, e.g. how is evidence for the actual runs of the system generated, how is it stored (and under which conditions) and how can it be checked for compliance? System operators should be able to trace system evidence from its generation all the way to its destruction, and know how to extract and present it in case of audits.

3.4.3 Accountability mechanisms in Ethical, Legal and Technical viewpoints

Accountability can be approached from three of the view points of the SALT framework: Ethical, Legal and Technical. Accountability requirements will vary depending on the viewpoint of the SALT framework involved: ethical, legal and technical.

3.4.3.1 Ethical viewpoint

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.[9] It is

[9] 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).

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.[10] 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.

Questions and recommendations contained in the SALT framework will focus on the way how surveillance system owners interact with the different stakeholders. By stakeholders we mean any individuals or group that can affect or are affected by the organisation's policies and/or actions such as data subjects (citizens), subcontractors (eg technology developers) or final users of the system (e.g. police).

As a way of example, questions include:

1. Have you identified who are your stakeholders (i.e. persons or groups that can affect or affected by the surveillance system you intend to deploy)?

- **Goal of the question**: Make the organization aware of who its stakeholders are and which types of commitments the organization have towards them. This is the first step to allow the organization to develop an accountability strategy.
- **Expected outcome**: The surveillance system owner identifies the stakeholders to whom the organization is accountable and their expectations.
- **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.
- **Best practice/Legal obligations:** 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. Have you opened channels of participation with the persons affected by the surveillance system (e.g. citizens)?

- **Goal of the question:** In order to increase the legitimacy of decision making, surveillance systems owners are advised to involve citizens in the decision of whether to deploy a new surveillance system, which technology or configuration is most likely to meet their

[10] Ibid.

expectations and to answer their needs and concerns. To achieve this goal, surveillance systems owners must open adequate channels of communications for each type of stakeholders targeted.

- **Expected outcome:** Surveillance system owners define which are the most appropriate channels to interact with citizens in order to understand their concerns (privacy or security related).
- **Information associated with the question:** Enabling participation of stakeholders is key for raising acceptance and legitimacy of the decision making process. Participation requires the active engagement of both internal and external stakeholders in the decisions and activities that affect them. At minimum, participation must include opportunities for stakeholders to influence decision making and not just the possibilities for approval and acceptance of a decision or activity. Participation strengthens ownership and buy-in for what organizations do by those they affect.
- **Best practice/Legal obligations:** Under the upcoming Data Protection Regulation, consultations of data subjects is also made mandatory in the context of Data Protection Impact Assessment. Article 33.4 stipulates that "*the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations*".

3.4.3.2 Legal viewpoint

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. The principle of accountability is introduced in the new European Data Protection Package, both in the draft General Data Protection Regulation and Law Enforcement Data Protection Directive[11], creating new obligations for surveillance system owners.

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. The outcome of the accountability mechanisms should serve to demonstrate the entity abides by the applicable legal framework.

Questions and recommendations contained in the SALT framework will focus on assessing whether surveillance system owners have implemented adequate procedural and technical safeguards to be able to demonstrate compliance with the legal framework.

[11] For a detailed overview of the measures implemented into the new European Data Protection Package, see PARIS Deliverable 2.1., p. 166-176. The amendments tabled by the Albrecht and Droustsas reports concerning the provisions on accountability have been voted by the European Parliament on 12 March 2014 and integrated in the texts under negotiations with the Council.

As a way of example, questions include:

1. Have you appointed a person responsible to check compliance with data protection obligations, such as a data protection officer?

- **Goal of the question:** Ensure that the organization has designated a person whose function is to supervise personal data processing activities**.**
- **Expected outcome**: The organization takes responsibility for ensuring that data protection obligations are met by allocating resources to supervision activities.
- **Additional information associated to the question**: Appointing a person responsible for supervising data processing activities eases personal data management and reporting to independent authorities such as Data Protection Agencies.
- **Best practices/Legal obligation**: Under the upcoming Data Protection Regulation, appointing a data protection officer becomes mandatory in the following cases:
    - the processing is carried out by a public authority or body
    - the processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period
    - the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects [eg video surveillance]
    - the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems

The data protection officer should have at least the following qualifications:

- extensive knowledge of the substance and application of data protection law, including technical and organisational measures and procedures;
- mastery of technical requirements for privacy by design, privacy by default and data security;
- industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed;
- the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation.

The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee.

Best practices: The Office of the Information and Privacy Commissioner of Canada, the region of Alberta and British Columbia have published guidelines to establish Privacy Management Programs which contain information related to Data Protection Officers and their role in an organization. The Guidelines, entitled “Getting Accountability Right with a Privacy Management Program” are available here.

The CNIL, the French Data Protection Authorities has also published guidelines to appoint a Data Protection Officer in compliance with the French data protection framework. These guidelines are available here.

2. Do you have an up-to-date catalogue of personal data processing activities?

- **Goal of the question**: Ensure that the organization has a catalogue of data processing activities and is aware and able to check their compliance with the legal framework.
- **Expected outcome**: The organization knows precisely which are its data processing activities.
- **Information associated to the question**: Creating a catalogue of personal data processing activities involves identifying the purpose of the data processing activity, the legal basis that legitimate this processing, the categories of data processed, security measures, authorized recipients of the data.
- **Best practices/legal obligations**: It is best practice to constitute a catalogue of data processing activities as part of the security measures implemented to ensure the security of data processing activities. It is usually considered as first step in privacy management programs to organize the supervision of the organization's practices.

As a way of example, under French law, the Data Protection Officer must maintain an up-to-date catalogue of data processing activities which contains the following information (art. 48 Decree n°2005-1309):

  - Name and address of the data controller
  - Purpose(s) of the data processing activity
  - Services in charge of deploying the data processing activity
  - Person and/or service in charge of receiving access and rectification requests from data subjects and their contact details.
  - Categories of data processed and categories of data subjects
  - Recipients or categories of recipients of the data
  - Retention period of the data

Under the upcoming Data Protection Regulation, data protection impact assessment should include a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller (article 33.3 a).

3.4.4 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 will focus on the nature of relevant evidence to facilitate the compliance checking process. This includes the choice of relevant categories of personal data and the processing operations that affect them. Moreover, privacy policies must be defined in a way that is explicit enough to allow for an encoding into a machine-readable format. Standardised privacy policy languages exist and should be used for this purpose. The SALT framework can help system designers by suggesting adequate privacy policy languages depending on the features of the surveillance infrastructure under consideration.

As a way of example, questions/recommendations include:

1. **Have you defined a data retention policy?**

- **Goal of the question**: Make the surveillance system owner aware of the need to delete information wherever not adequate or relevant for the purposes of the processing.
- **Expected outcome**: The data are not kept longer than necessary for the purposes of the data processing activity. Special safeguards are implemented to enforce these policies.
- **Information associated to the question:** Personal data should not be kept any longer than strictly required for the purposes of the processing. After that, data should be deleted.
- **Best practices**: The maximal period of time for which a category of personal data may be kept should be linked to an aspect of the information system which can be automatically analysed, e.g. system logs mentioning data deletion.

Retention period might be defined based on legal obligations. For instance, video surveillance data cannot be kept for longer than one month under French Law (Art. 10 Act n°95-73).

3.4.5 Accountability mechanisms in the SALT process

Accountability mechanisms can be implemented at different stages of system design in line with the functional approach described in D.2.2, section 2.1.1**.**

3.4.5.1 Step One: Intention

Before system design, at the stage of "intention", accountability mechanisms will be concerned with improving the level of answerability of the surveillance system owner towards its stakeholders. 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.

As a way of example, questions include:

1.Have you organised a consultation process with the citizens that will be affected by the surveillance system in place?

- **Goal of the question:** Ensure that surveillance system owners are aware of the concerns of the citizens.
- **Expected outcome**: Surveillance system owners consider the option of actively involving their stakeholders.
- **Information associated to the question:** n/a
- **Best practices/ legal obligations:** Under the upcoming Data Protection Regulation, consultations of data subjects is also made mandatory in the context of Data Protection Impact Assessment. Article 33.4 stipulates that "*the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations*".

3.4.5.2 Step One bis: Checking national requirements

National legal framework can integrate specific obligations with regards to accountability mechanisms. For instance German Data Protection Law require private entities to appoint a data protection officer whenever there are more than nine persons permanently engaged in automated data processing or at least 20 persons engaged in non-automated processing. Under French law, the appointment of a Data Protection Officer is voluntary but relieves the company from a series of obligations (e.g. notification obligations for non-sensitive data processing activities).

Questions and recommendations contained in the SALT framework will focus on the national requirements to implement specific accountability mechanisms or reporting obligations.

As a way of example, in the case of France, questions/recommendations would include:

1. Have you appointed a Data Protection Officer?

- **Goal of the question:** Make data controllers aware of the possibility to appoint a data protection officer

- **Expected outcome:** Make data controllers aware of the benefits of appointing a data controller officer even if not mandatory.
- **Information associated to the question**: The French data protection framework provides for the possibility to appoint a Data Protection Officer (article 22 of Act n°78-17 and articles 42 to 56 of Decree 2005-1309). Even if not mandatory, this relieves the entity from a series of obligation, most particularly in terms of notifications of non-sensitive data processing activities.
- **Best practices**: The CNIL, the French Data Protection Authority has published guidelines about the role and qualification of the Data Protection Officer under French Law. The guidelines are available in French here. Most particularly, appointing a Data Protection Officer is regarded as a guarantee for compliance with the legal framework (the DPO is in charge of ensuring such compliance), for data security (one function of the DPO is to ensure that all required measures have been taken to ensure such data security), a way to ease the administrative burden over data controllers in terms of notifications, a way to ensure a preferred collaboration channel with the CNIL (as specific communication channels are made available to DPOs), a way to show data controller's commitment to respect privacy, a tool to valorize data as asset or the company as long as the DPOs should ensure the reliability of the data processed and thus facilitates further data sharing in compliance with the legal framework.

3.4.5.3 Step Two: Integration of considerations

During system design, accountability mechanisms will focus on identifying mechanisms that will enable further reporting and verification of the actions performed on the personal data and whether these match the surveillance system owners' policies, once the system is deployed.

Questions and recommendations contained in the SALT framework will focus on ensuring that system includes adequate verifiability mechanisms.

As a way of example, questions/recommendations include:

Have you established an audit trail to trace actions performed over the personal data?

- **Goal of the question:** Make the surveillance system owner aware of the benefits of incorporating traceability mechanisms
- **Expected outcome:** The surveillance system owner implements traceability mechanisms into the system.
- **Information associated with the question:** In the context of information security, accountability refers to the ability to ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. Implementing accountability requires an effective audit trail, which are audit records that enable the monitoring, analysis, investigation, and reporting of information system activities. Implementing accountability requires an effective audit

trail, which are audit records that enable the monitoring, analysis, investigation, and reporting of information system activities.

Common mechanisms for establishing audit trail are to use logging and monitoring services provided by computer systems. A log is a record of the events occurring within a network and system. Logs are composed of log entries. Each entry contains information related to an event that has occurred within a system or network. As records of events, log files provide basic data of the user activities in a system. The audit mechanisms such as audit process and actions performed by machines and humans can use the log files as an input and process the files into meaningful information for accountability.

- **Best practices:** In the field of video surveillance, implementing an audit trail is an effective means on the technical level to provide accountability in video surveillance system. Since logging is the primary mechanism to establish audit trials, several issues related to log management need to be considered in the context of video surveillance system. The National Institute of Standards and Technology has published a Guide to Computer Security Log Management [NIST800-92] pointing out some the challenges included in log management:
  - log generation and storage that entails issues of
    - multiple logs from heterogeneous sources, as well as multiple logs generated from a single source,
    - log content inconsistences caused by different log entry formats across different hardware and software;
  - log protection against unauthorized tempering and deletion.

3.4.5.4 Step Three: overall assessment and system lifecycle

After system design, the system must be improved whenever weaknesses are identified. For example, accountability mechanisms would have to be improved in case of the data breach if the system is not able to provide information on the data affected and the attack suffered by the system. Similarly, if the surveillance system owner receives a large number of complaints from data subjects without being able to answer, it should provide for more efficient complaint mechanisms.

This part does not call for specific questions or recommendations. Rather, whenever the surveillance system owner identifies a point of concern, it must come back to the initial questionnaire to identify the weaknesses of the system deployed and to work out possible solutions.

4 Conclusions

This document provided guidelines for SALT users, i.e. the people in charge of applying the SALT frameworks. It has provided tentative guidelines for future users of SALT framework, mostly SALT system designers and SALT system owners. Guidelines here have been 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 the introduction, we explained what can be expected out of those guidelines, what are their purpose in terms of facilitating the appropriation and use of SALT frameworks by SALT users. We explained why it makes sense to adopt a domain approach for users.

In section 2, “Concepts of SALT frameworks for users”, we introduced the main concepts used in SALT frameworks in an easy and understandable way, so that SALT users may easily apprehend what SALT framework are about, what they deal with and what they encompass. We explained how it encompasses the socio-contextual and ethical, legal, technical and accountability dimensions and how all of this fits in the more general figure of SALT process. Then we got more into details into the three-stage process, which finds that SALT systems are put into place sequentially. In this respect, we identified three stage of development of a surveillance system into public space: conception, design and implementation. Lastly, we introduced the guidelines and their definition, their purpose, and the extent to which they will be useful for SALT users.

In section 3, we then introduced the guidelines *per se*, domain by domain. We dealt with the socio-contextual and ethical dimensions, and suggested a certain amount of guiding principles for applying SALT frameworks under these dimensions. Then, we 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. We coped with the technical dimensions, identified the relevant technical users and provided step-by-step guidelines which will take him/her through the development process. Lastly, we examined the accountability dimension. This dimension crosses many aspects of both the socio-contexual and ethical, legal and technical dimensions. Since it rests at the intersection of both three sections, it appeared useful to wrap up SALT procedures and to fully complete SALT Framework so as to make them truly comprehensive.

In the future, those guidelines will be updated and will fit the actual use case scenarios which will be developed in the next phases of the project. For the moment, they are still narrowly associated with SALT concepts which are very abstract in scope. So the guidelines should evolve according to how they play out concretely in the cases of biometry and videosurveillance.

Among those coming evolutions, it must be said that future guidelines will include feedback mechanisms for users so as to enhance the guidelines of the system also, depending on how helpful is their experience of the SALT framework and how they see it would be possible to improve its methodology.