PrivAcy pReserving Infrastructure for Surveillance

Deliverable D6.2

Biometrics Use Case SALT Compliant Framework

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D6.2
Title:	Biometrics Use Case SALT Compliant Framework
Version:	v1.0
Date:	7/1/2015
Confidentiality:	Public

Contributors: R. Alonso, V. Hidalgo & M. Saornil (VT)
Francisco J. Rodríguez (UMA)
Fanny Coudert & Lina Jasmontaite (KUL)
Claire Gayrel & Nathalie Grandjean (UNamur)
Daniel Le-Metayer & Vinh-Thong Ta (INRIA)

Funded by the European Union's Seventh Framework Programme

Table of Contents

Document History

Version	Status	Date
v0.1	First draft of ToC	11/9/2014
v0.2	Contribution to section 2.1 (VT)	12/11/2014
v0.3	Section 2 updated (VT); Contribution to sections 3 and 4 (UNamur, KU Leuven, INRIA, VT)	4/12/2014
v0.4	Contribution of UNamur added to section 3; revision of sections 3.4 & 3.5 by INRIA; Contribution to sections 5.1 & 5.2 by VT	16/12/2014
v0.5	Contribution to section 5 by UMA	16/12/2014
v0.6	Revision of section 3 by KU Leuven; update of section 3.2 by UNamur; contribution to section 1, and reorganization of contents by VT;	18/12/2014
v0.7	Update of section 5, and minor corrections by VT	19/12/2014
v0.8	Revision and minor corrections by Thales	23/12/2014
v0.9	Revision and minor corrections by Trialog	31/12/2014
v1.0	Final version	7/1/2015

Approval		
	Name	**Date**
Prepared	VT, UMA, UNamur, KU Leuven & INRIA	19/12/2014
Reviewed	Thales & Trialog	31/12/2014
Authorised	VT & Trialog	8/1/2015

Circulation	
Recipient	**Date of submission**
Project partners	8/1/2015
European Commission	8/1/2015

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
AEPD	Spanish Data Protection Commissioner's Office *(Agencia Española de Protección de Datos)*
AP	Authorized Person
APDB	Authorized People Database *(biometric template database)*
API	Application Programming Interface
BS	Biometric System
DC	Data Controller
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DS	Data Subject
ICT	Information and Communication Technologies
IN	Installer
LA	Local Authorities
LOPD	Spanish Organic Law 15/1999 of Personal Data Protection
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PIR	Passive Infrared
PMP	Privacy Management Program *(privacy policy)*

PO	Police Officer
RDB	Results Database
RIS	Re-Identification Server
RMS	Results Management Server
SA	System Administrator
SALT	Socio-ethical, Legal, Technical
SD	System Designer
SDV	System Developer
SF	SALT Framework
SO	System Operator
SP	System Proposer
SSP	Surveillance Service Provider
UAP	Unauthorized Person
VPU	Video Processing Unit

Executive Summary

The main goal of the PARIS project is the definition and demonstration of a methodological approach for the design of surveillance systems optimizing the surveillance capabilities together with privacy protection and integration of the concept of accountability. For this reason, we define a framework called SALT (Social, ethicAl, Legal and Technical), and two use cases for its demonstration.

This document covers the work of task T6.3, in which the SALT Framework is adapted for the evaluation and design of biometric systems, taking the use case described in D6.1 as an example to show how the different concerns on privacy and accountability can be integrated in the design of surveillance systems using the methodologies developed in this project.

1 Introduction

This document aims at describing how the SALT Framework can be used for the design of biometric systems in order to take into account privacy and accountability from the start, identifying for this the elements of the SF that are more relevant for biometrics. This task has been performed through the implementation of the methodologies developed so far in this project (WP2-WP4), and using the biometrics use case defined in WP6 as an example.

The different evaluations of the biometrics use case, made necessary to update the description of the system, included initially in D6.1, and to provide more detailed information about the stakeholder problems and how are they going to be addressed *(Section* 2*: Biometrics use cases and scenario).*

The results of the work done in WP2 have been applied to the biometrics use case presented in this document, allowing to make an in depth privacy and accountability assessment of the system under development, and to identify the main socio-ethical, legal and technical concerns that should be pointed out by the SALT Framework *(Section* 3*: Privacy and Accountability concerns)*.

Section 4*: Artifacts* summarizes the set of socio-ethical, legal and technical mechanisms and procedures that are going to be implemented in the biometric use case to address the concerns of *Section* 3*,* to ensure that the general recommendations on privacy and accountability are taken into account.

Finally, *Section* 5*: SALT Framework specialized for biometrics* reviews the different resources provided by the SALT Framework, that can be used during the different stages of the system lifecycle for the assessment of systems in terms of privacy and accountability, and also to design, develop and maintain a biometric system that balances surveillance with privacy.

All this work has served not only to refine the biometric use case, but also to improve the methodologies developed in this project. This work will continue during the next months of the project, and the final results will be included in subsequent deliverables of WP2-WP6.

2 Biometrics use cases and scenario

In WP6, to demonstrate how the SALT Framework can be used to integrate privacy and accountability in surveillance systems (as stated in D6.1), we have defined a use case for the **detection of unauthorized accesses to a building with security requirements preserving users' privacy**. The main objective of the system under development is to facilitate the work of security operators and the collection of evidences for law enforcement in case of intrusion. To achieve this goal, the system includes a mechanism for the re-identification of people that uses an innovative biometric technology *(bodyprints)*.

After the privacy impact assessment performed through the first version of the questionnaire for biometrics developed in this project, we have decided to update the system architecture. Besides, we have added more detailed information about the use case that is necessary to justify the necessity and legitimacy of the system.

2.1 Scenario description

2.1.1 Stakeholder needs

The stakeholder company is Visual Tools (VT), that requires a solution to protect all the material stored in their headquarters located in Madrid (Spain). Not only expensive hardware equipment is stored at the VT's premises (e.g. video surveillance products, processors, servers), but also software applications, developed or still under development, that are subject to intellectual rights protection, and that require huge investments in terms of time and human resources.

Figure 1: Selected scenario

The company headquarters have a total area of approximately 1000 m^2 distributed on three floors, with two entrances from the street that are not shared with other dwellings or offices. There are also many windows at street level, that could be smashed to break in.

There is a video surveillance system already installed at the mentioned premises, but as the area to monitor is large, and the cameras have to be set up in a way they do not obtain images from the street, there are many corners not covered by the system. Moreover, in case of robbery, with the current system, it is quite complicated to find the video sequences to be provided as evidences to the police. Without a clue about the exact moment of the incident, the operator has to search through many hours of video content from all the cameras.

The existing security measures also include an alarm system that uses Passive Infrared motion detectors (PIR), which is connected to the control center of a security company contracted for monitoring the facilities. In case of alarm, the security company tries to contact the person of Visual Tools registered as responsible for the system, who is in charge of verifying the alarms by connecting to the video surveillance system or by going in person to the office. If it is not possible to communicate with anybody from VT, or if there is any suspicion of robbery, the security company calls the police to request dispatch to the office immediately.

The main problem with this system is that there are maintenance employees cleaning up the premises five times per week at night, and while they work the alarm system has to be disconnected to avoid false alarms. False alarms can have a significant negative impact on both the stakeholder and the service provider, as they can cost a lot of money in fees, and they can also create dissatisfaction with the system implemented, as well as with the security provider.

Anyway, with the current security system, processors and other material have been stolen from the office, which seems to have occurred at night, and therefore the company wants to improve the security to prevent such losses in the future.

In short, the solution designed should fulfill the following requirements from the stakeholder:

1. Prevention against theft (deterrence)
2. Facilitation of the work of security guards, reducing the false alarms
3. Facilitation of the collection of evidences for law enforcement

2.1.2 Proposed solution

To address the stakeholder needs we propose a biometric system based on video analysis that is capable of detecting unauthorized accesses in the scenario defined. The system will cover the main transit areas of the office with cameras, providing depth and spatial information that will be analyzed to detect the people accessing to the office. It will also include a mechanism for re-identification allowing to match any person detected with a database of authorized people. In case the system does not recognize the person detected, an alarm will be generated and displayed to the operator responsible for monitoring the facilities.

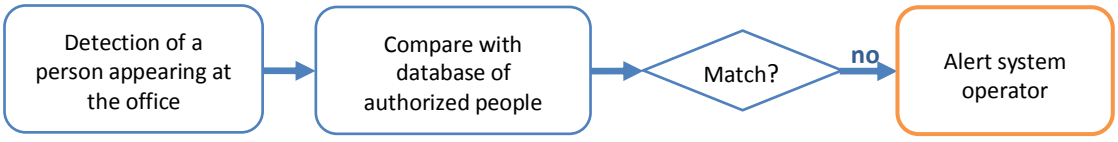

Figure 2: Summary of the functioning of the proposed system

These are the main features provided by the system that will serve to solve the stakeholder problems:

- Re-identification capability, allowing to compare any data subject with a database of authorized people.
- Management tool displaying the results of the re-identification process, that can be used by security operators to react earlier in case of intrusion, and also to discard false alarms more easily.
- Collection of information of any access detected, such as the date and time, which will facilitate the video search in case of incident, and therefore the provision of evidences to local authorities.

In the scenario described, the authorized people are the maintenance employees, and the detection period, in which the biometric system will be operating, is defined from 9:00 PM to 7:00 AM. The current alarm system will still be used during the night, but while the maintenance staff are cleaning the facilities, only the biometric system will remain switched on.

2.2 Biometric technology

The proposed biometric system uses **bodyprints** for the re-identification of people. A bodyprint is a vector of features of a person that uses physical characteristics, such as the height and width of a person and the color of his/her clothes, which are sufficiently distinctive to allow identifying and discriminating people, even with similar clothes.

In the scenario described, the authorized people are the maintenance employees that wear uniforms or clothes with a particular color, which eases their identification.

The process of extraction of bodyprints can be summarized as follows:

1. The data provided by the cameras is continuously being analyzed in order to detect new people appearing in the scene.
2. A person is detected.
3. That person is tracked during different video frames.
4. With the information of the spot that the person leaves in the different frames, the bodyprint is created.

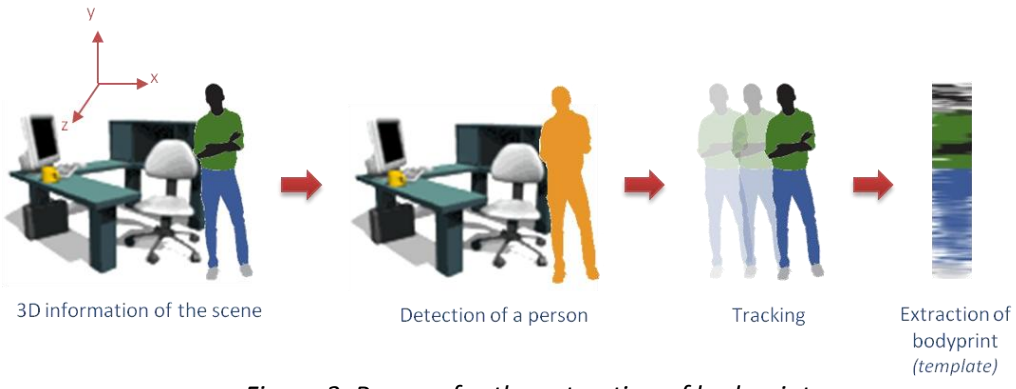

Figure 3: Process for the extraction of bodyprints

It is a process that does not require the collaboration of the individual, as the samples are obtained automatically by the cameras from a certain distance, and that does not require special light conditions.

The data collected for every person detected by the device extracting bodyprints are :

- **.dlm*: these files are used for the detection and tracking processes.
- *keyImage.jpg*: this image is stored for verification purposes, to easily check to whom the bodyprint belongs.
- *t_mean_time.tif*: this is the bodyprint extracted for the person detected, that does not identify directly that person as can be seen in the image of the example.

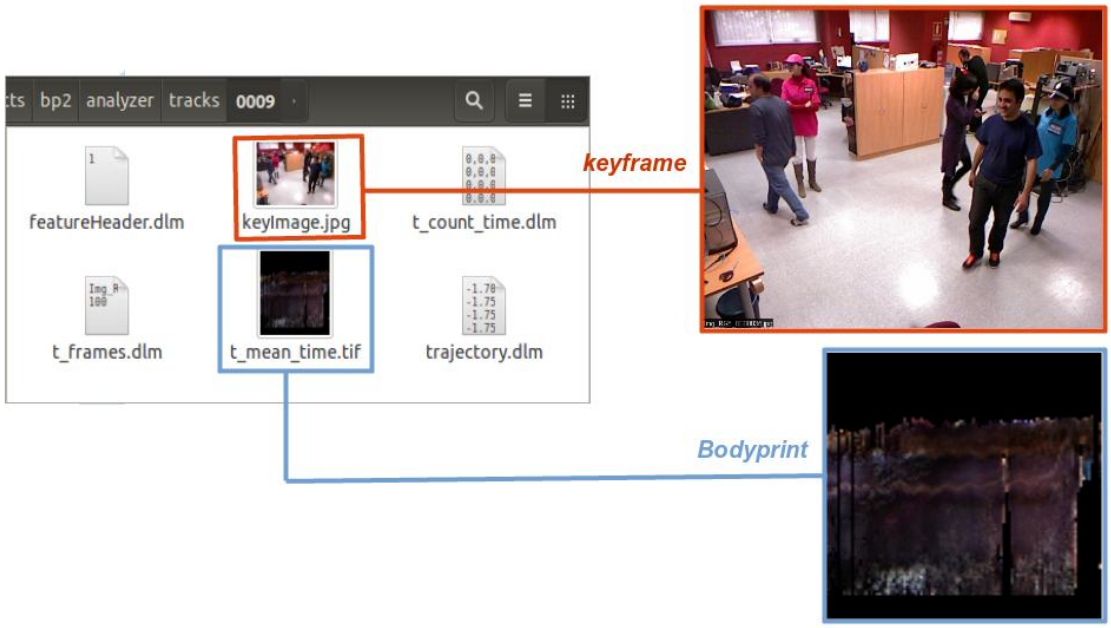

Figure 4: Results of the extraction of bodyprints

It is important to emphasize that the bodyprints in this system will not be linked with any other personal information, and that although the bodyprints are generated from biometric data of the individuals, they cannot be used to reconstruct neither the images nor the biometric features processed for its creation. To identify a person through a bodyprint it is necessary to use the biometric system.

Moreover, the bodyprints depend on the clothes worn by the data subject, thus a bodyprint can be used with the biometric system to identify a person only if that person has not changed significantly with respect to the moment when the stored bodyprint was extracted. This makes necessary to update periodically the bodyprints of the template database.

2.3 System overview

2.3.1 System components and architecture

We have updated the system architecture after the privacy impact assessment performed. The main difference with respect to the system described in D6.1 is the separation of the management of the results from the matching process, in order to increase the security of the template database. The new configuration of the system is then composed of the following elements:

- **Video Processing Unit** (VPU). This device is continuously analyzing the images from the depth cameras connected to it to extract the bodyprints of the people appearing in the scene. For each depth camera used, a VPU is required.
- **Re-Identification Server** (RIS), which periodically requests the new bodyprints from each VPU unit installed in the system. Anytime a new bodyprint is obtained, the RIS performs the matching with the template database. The results are temporary stored in the RIS and copied to a directory of the RMS. This server does not have connection to the Internet.
- **Results Management Server** (RMS), which is responsible for managing the alarms and displaying the results to the system operator through a Web UI accessible from a remote location.
- **Authorized People Database** (APDB): template database containing the bodyprints of the people that are authorized to be inside the office at the defined period.
- **Results Database** (RDB): database containing the results of the matching process and the alarms generated.

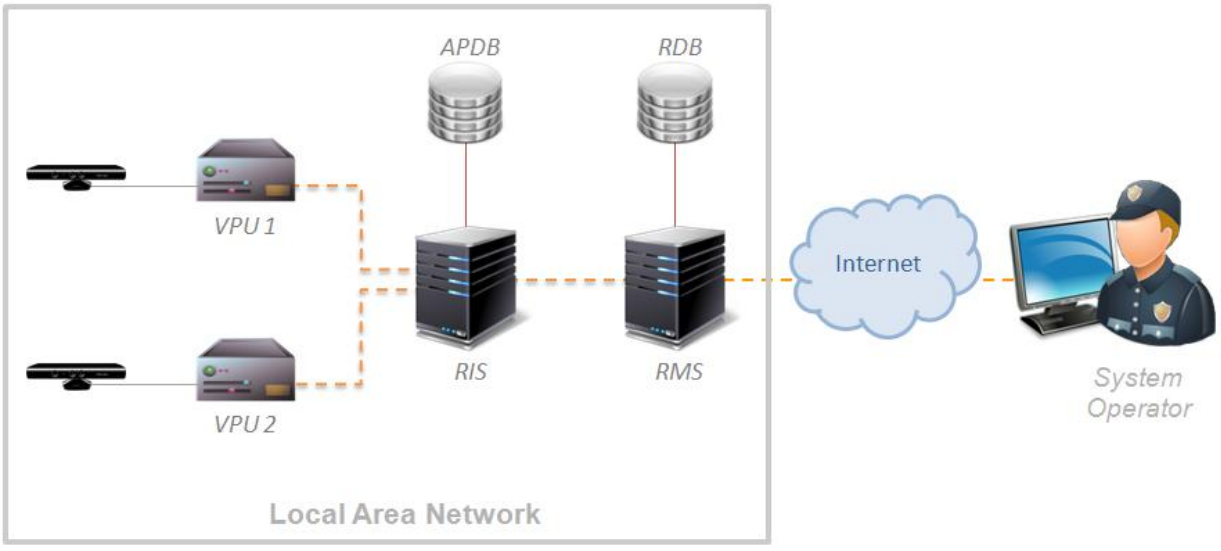

Figure 5: System overview

All the devices are connected through a **local area network** installed in the Visual Tools premises, and only the RMS is connected to the Internet, thus it will only be possible to access the other components from the office (VPU, RIS, APDB and RDB). If it is required for auditing purposes, remote access to a specific unit can be temporary provided, but always to an authorized person and for a specific and justified purpose.

2.3.2 System users

These are the users of the system involved during the process of detection of unauthorized people:

User	Abbreviation	Main tasks
System Administrator	SA	Main responsible for the system, dealing with these tasks: • Authorizing the access to the system and creating new system users with the adequate privileges. • Enrolment of authorized people in the system. • Configuration and management of the system.
System Operator	SO	• Monitoring the system during the detection period defined, to check that the VPUs are working correctly and to review the results of the matching process in the RIS. • Verification of any alarm generated by the system. • Reporting the incidents to the local authorities.

Table 1: Main system users

Besides, these other users may require access to the system:

User	Abbreviation	Purpose of the access
Data Protection Officer	DPO	Audit the system to verify its compliance with the current regulations on privacy and data protection.
Police Officer	PO	Get evidences of an unauthorized access for law enforcement.
Data Subject	DS	Check his/her personal information stored in the system.

Table 2: Additional system users

2.3.3 General system operation

The process of detection of unauthorized people is performed in two phases: enrolment and matching.

2.3.3.1 Enrolment

In this phase, the *bodyprints* of the authorized people are extracted and stored in the system. This task is managed by the *System Administrator (SA)*.

The process of enrolment is performed in three steps:

1. *Capture information*: A video of the authorized person is recorded using a depth camera. This task requires the collaboration of the person to be enrolled in the system. As a result, a video sequence containing images of the data subject is obtained.
2. *Extraction of bodyprints*: For each video, several bodyprints will be extracted, and a specific user interface will facilitate the selection of the most adequate for the matching phase.
3. *Store bodyprints in the APDB*: This task is performed manually by the *System Administrator*.

The enrolment is *offline*, meaning that steps 1-2 are not performed necessarily one right after the other, as it is possible to record all the videos from the authorized people first, and process them in another moment.

As the bodyprints are not very stable in time, it will be necessary to repeat the enrolment process periodically (e.g. once every six months) in order to ensure the accuracy of the system.

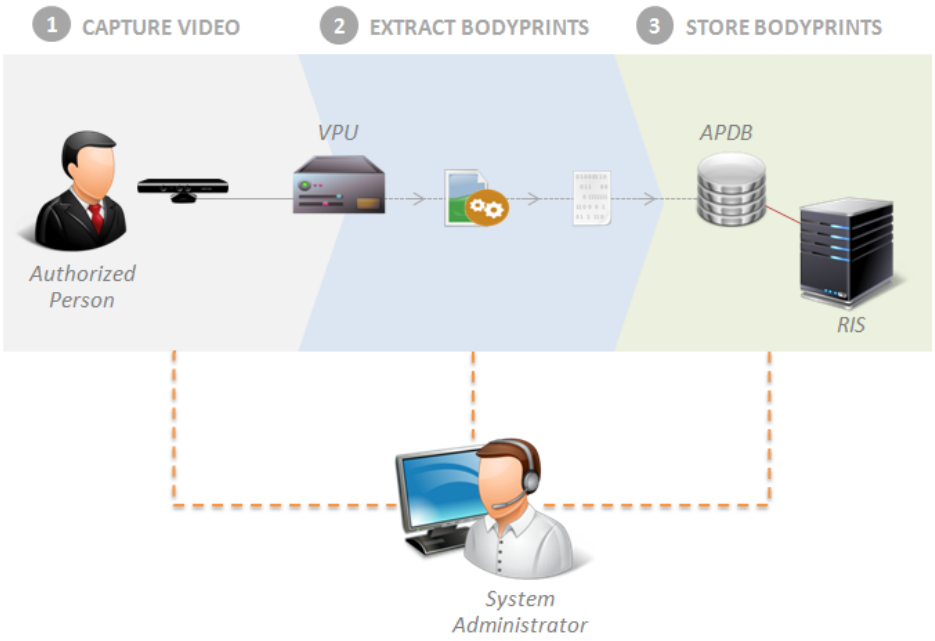

Figure 6: Enrolment process

2.3.3.2 Matching

The goal of this phase is the detection of unauthorized accesses to the office under surveillance in the period defined.

The matching process is carried out automatically by the system during the detection period, and monitored by the *System Operator* (SO), who is responsible for the management of the results. It is composed of the following steps:

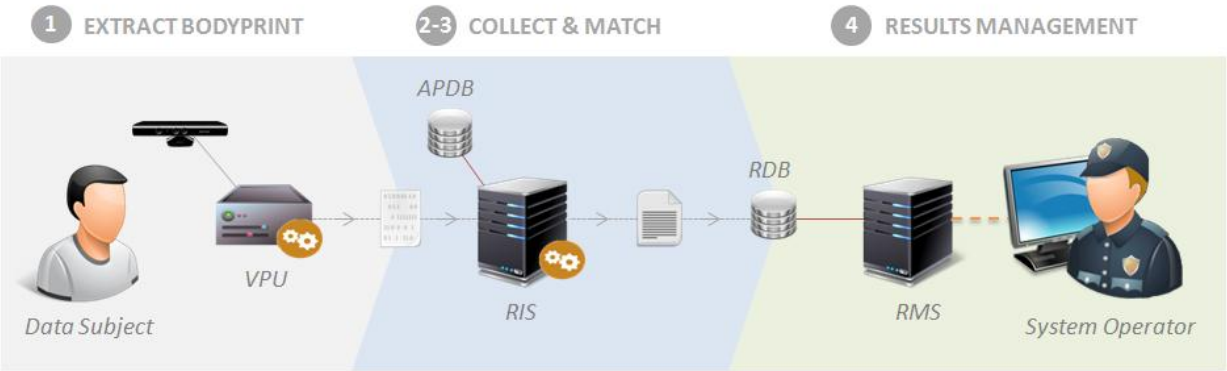

Figure 7: Matching process

1. *Extraction of bodyprints*: Each VPU continuously captures images of the scene and automatically analyzes them to obtain the bodyprints of the people detected.
2. *Collection of bodyprints*: The RIS periodically requests the new bodyprints to the VPUs using the corresponding REST API.
3. *Matching*: The new bodyprints are compared by the RIS with the templates stored in the APDB. The results of the comparison are copied to the Results Database (RDB).
4. *Results management*: The Results Management Server (RMS) displays the information stored in the RDB to the SO, showing alerts in case an unauthorized access is detected. The SO connects to the RMS through a specific user interface and checks the alerts. In case of intrusion, the SO is responsible for reporting the incident to the local authorities.

Although the final objective of the matching phase is the classification of people appearing in the scene as authorized or unauthorized, the recognition process is performed through the identification of people: if the template of a new data subject matches any of the templates of the APDB it is considered authorized, otherwise, the data subject is marked as unauthorized and an alarm is generated. Therefore, the biometric system is used for identification.

2.3.4 Data management

2.3.4.1 General procedures

For the correct functioning of the system, it is necessary to configure the **detection period** and the **system users**, that are created by the SA with restricted access to the information stored in the system.

All the devices will include access control mechanisms to let only a certain group of users have access to the system (any user authorized by the SA):

- *VPU*: the SA is allowed to access the VPU, and also any other user authorized by the SA for auditing purposes. Besides, the API for the collection of bodyprints will require authentication and authorization, being the RIS and the SA the only users allowed to request information.

- *RIS*: the SA is allowed to access the VPU, and also any other user authorized by the SA for auditing purposes. If any data subject require access to his personal information stored in the system (APBD), the SA will have to authorize, register and supervise that access.
- *RMS*: the user interface displaying the results of the matching process and allowing to manage the alarms, will be protected by access control mechanisms. The users allowed to see this information are the SA, the SO, and any other user authorized by the SA for auditing purposes or for law enforcement.

Moreover, all the sensitive information that can be stolen or misused will be properly protected.

2.3.4.2 Enrolment phase

This is the data collected during the enrolment phase:

- **Videos of the people to be enrolled in the system**. These videos are captured from the depth cameras with a specific user interface available in the VPUs, and they can only be accessed by the System Administrator. Once recorded, the videos are encrypted and stored in one of the VPUs, until they are analyzed and the corresponding bodyprints are extracted. After that, the videos are removed from the system. In any case, the videos will be kept for a maximum period of one month as established by the Spanish Law.
- **Bodyprints of the authorized people (APDB).** During the enrolment process, all the bodyprints obtained for the person to be enrolled are temporary stored in the system. It will be possible to select the most adequate candidate for the matching phase with a specific user interface, after which, the bodyprint selected is copied by the SA to the APDB and the discarded bodyprints are removed from the system.

  By just storing the bodyprints (*t_mean_time.tif)* it is possible to perform the recognition of individuals, but to facilitate the evaluation and the refinement of the system, for each person enrolled, the APDB will include a folder with the selected bodyprint, the files extracted from the detection/tracking process and the key frame.

2.3.4.3 Matching phase

During the detection period, this is the data managed by the system:

- **Video frames.** The images from the depth cameras installed in the office are continuously being captured by the VPUs. These images are processed on the fly, which means that the video frames are directly analyzed and no video sequence is stored during the matching phase. There are two main processes running in the VPUs to extract the bodyprints from the video frames: a first process captures the data from the depth cameras and sends it to a shared memory; a second process reads the information of each video frame from the shared memory and analyzes it, and once finished with a frame it is released from the shared memory, and the next frame is loaded.

- **Temporary Bodyprints (VPU).** The results of the image processing are temporary stored in the VPUs. As mentioned before, for each person detected, a folder with the results of the detection/tracking processes is stored, a key frame and also the date and time when the corresponding person was detected in the scene *(detection timestamp)*. The RIS requests periodically these new bodyprints, and once sent to the RIS, the complete folder with the temporary results is removed from the VPU device.
- **Temporary Bodyprints (RIS).** The RIS compares any new bodyprint collected with the APDB. Once compared, the bodyprints are temporary kept in the system until the results are validated by the SO.
- **Results of the comparison (RIS).** All the results of the comparison performed in the RIS are stored there, including all the parameters obtained in the matching process (e.g.: level of confidence of the results), which will serve to detect incorrect configurations of the re-identification module. Besides, the classification of the user (authorized or unauthorized) and the detection timestamp are copied to the Results Database (RDB) to be displayed to the SO.
- **Results of the comparison (RDB).** The only data stored in the RDB, obtained from the matching process, are: the final result of the comparison (person authorized or unauthorized), the date and time when that person was detected (timestamp), and the key frame associated to that person. This information will be displayed to the SO through a specific user interface so that the SO can check the alarms. The positive results, as well as the false alarms, will be removed from the RDB once verified. Any result associated to an alleged unauthorized access will be kept as evidence for the local authorities.
- **Key frames (VPU/RIS).** These images are obtained in the VPUs for each person detected and sent to the RIS with the corresponding bodyprints. Once sent to the RIS, they are removed from the VPU. After that, they are copied to the RMS to facilitate the verification of alarms by the SO or by the local authorities in case of intrusion. Once sent to the RMS, they are removed from the RIS. In any case, the images will be properly protected so that only the authorized users can have access to them (SA, SO and local authorities).

2.4 Use cases

In this section a summary of the use cases defined in D6.1 are presented. They have been reviewed and updated, in particular some of the actors and procedures have been refined.

2.4.1 Use Case I: Design of a SALT compliant biometric system

The goal of this use case is the demonstration of how the SALT Framework can be used for the design of a biometric system.

1. A company requires a video surveillance system for the detection of unauthorized people in the selected scenario. As this company will be the one using the system once deployed, it will be hereinafter referred to as *Data Controller*.

2. The *Data Controller* delegates the task of elaborating the specification of the system to one of their employees or to an external consultant with knowledge in the areas of security and surveillance systems, that will take the role of the *System Proposer*.
3. The *System Proposer* collects the requirements of the system from the *Data Controller*, and, in this case, he will use the SALT Framework to get some concerns and recommendations regarding privacy and accountability according to the needs of the client to complete the system specification.
4. The *System Proposer* is normally responsible for finding a company providing the required surveillance service according to the developed specification *(Surveillance Service Provider)*.
5. The *Surveillance Service Provider* entrusts the design task to the *System Designer*.
6. The *System Designer* elaborates a design of the system following the specification given by the *System Proposer* and the business constraints imposed by the *Surveillance Service Provider*.
7. Once a design is created, the *System Designer* can use the SALT Framework to validate the design according to the associated concerns. The SALT Framework will highlight the concerns not addressed, if any, so that after an iterative process of design and validation, a SALT compliant design is obtained.

In the demonstrator, Visual Tools takes the role of all the companies, being at the same time the *Data Controller*, the *System Proposer* and the *Surveillance Service Provider*.

2.4.2 Use Case II: Deployment of a SALT compliant biometric system

This use case is focused on showing how the system is set up and which people is involved during this process and also during an audit for accountability issues.

1. The *Surveillance Service Provider* entrusts the development task to the *System Developer*.
2. The *System Developer* implements the system according to the design elaborated by the *System Designer*.
3. Once the system is developed and tested, the *Installer* sets up the surveillance system in the *Data Controller*'s facilities and gives access to the system to the *System Administrator* for management.
4. The *System Administrator* defines the detection period in the different devices and creates a system user with restricted privileges for the person responsible for monitoring the office *(System Operator)*.
5. At any moment, the *Data Protection Agency* may require the verification of the compliance of the system with the current regulations. In that case, the *Data Protection Officer* in charge of this task, requests information of the system deployed to the *System Administrator*.

6. The *System Administrator* collaborates providing the information requested and also access to the system when necessary. Any access to the information stored in the system is traced.
7. The *Data Protection Officer* may also require access to the SALT Framework to review the SALT references used to design and develop that specific system.

2.4.3 Use Case III: Detection of unauthorized people

This use case serves to demonstrate how the system is used once it is operational, and particularly how the surveillance service is provided according to the SALT guidelines.

1. The *System Administrator* enrolls in the system the group of employees that are allowed to access the office at the defined period. From this moment onwards, the system is ready for the detection of unauthorized people.
2. The *Biometric System* works in the defined period detecting and categorizing the people appearing in the scene. This process is monitored by the *System Operator*.
3. Anytime an *Unauthorized Person* is detected, the *Biometric System* generates an alarm that is displayed to the *System Operator*.
4. The *System Operator* verifies the alarms generated and reports the incidents to the *Local Authorities*.
5. A *Police Officer* is sent to collect information of the incidents in order to take the adequate measures for law enforcement. For this, the *Police Officer* may request to have access to the information stored in the system, for which the authorization of the *System Administrator* is required. Any access to the information stored in the system is traced.

2.4.4 Summary of actors and roles

Actor	Abbreviation	Role	Other names
Data Controller	DC	Person requiring the surveillance system, and owner of the facilities where it is going to be installed. It is normally a company.	*System Owner, Infrastructure Provider, Client*
System Proposer	SP	Person/company responsible for the elaboration of the specification of the system according to the Data Controller's needs. This person is sometimes an employee of the Surveillance Service Provider company, but he can also be an independent consultant hired by the Data Controller. ** User of the SALT Framework to get concerns about privacy and accountability.*	
Surveillance	SSP	Company providing the surveillance	*Service Provider,*

Service Provider		service. This company adds a set of business constraints to the specification of the system.	*Technology Provider*
System Designer	SD	Person (or team) responsible for the design of the system taking into account the given specification and the business constraints of the SSP. This person is normally an employee of the SSP, but this task could be outsourced to an external company. ** User of the SALT Framework to validate the system designed, and also to consult references.*	*Engineer*
System Developer	SDV	Person (or team) responsible for the development of the system according to the design created by the SD. This person is normally an employee of the SSP, but this task could be outsourced to an external company.	*Engineer, Development Team*
System Administrator	SA	Person responsible for the management of the system once it is operational for the surveillance service. The SA is normally an employee of the Data Controller.	
Installer	IN	Person responsible for the deployment of the system in the Data Controller's facilities.	*Engineer*
System Operator	SO	Person responsible for monitoring the facilities of the Data Controller, that uses the surveillance system tools during the matching phase to check unauthorized accesses to the office.	*Operator*
Data Protection Authority	DPA	Authority charged with data protection, assumed the role of the supervisory authority for a country. It is equivalent to a national data protection commissioner.	
Data Protection Officer	DPO	Employee of the DPA responsible for verifying the compliance of the surveillance system with the current regulations on privacy and data protection.	
Biometric System	BS	Video surveillance system using biometric technologies for the detection of unauthorized people at the office.	
Data Subject	DS	Individual whose biometric data has been captured by the biometric system.	

Authorized Person	AP	A person that is in the Authorized People Database (enrolled in the system).	
Unauthorized Person	UAP	A person that is not in the Authorized People Database.	
Local Authorities	LA	Entity responsible for social order, public safety and law enforcement.	*Law Enforcement Agency*
Police Officer	PO	Agent of the LA in charge of the investigation of the incidents *(unauthorized accesses)*.	

Table 3: Use Cases - List of actors

3 Privacy and Accountability concerns

In this section we have carried out an evaluation of the impact on privacy of the biometric system proposed in WP6, with the objective of extracting the main privacy and accountability requirements that the system shall fulfill, and that should be pointed out by the SALT Framework. This evaluation is based on the **three stage design process** developed in WP2, which is summarized later in section 5.1, and it serves to complete the work started in D6.1 with the extraction of more specific requirements for the updated version of the biometric system through the use of the tools and guidelines developed so far in WP2:

- The SALT questionnaire for biometric systems developed in this project, that is going to be integrated in the SALT Framework, whose current version covers some legal and technical aspects.
- Socio-ethical assessment based on the work of D2.2, providing additional socio-ethical concerns not integrated yet in the SALT questionnaire for biometrics.
- Spanish legislation, providing guidance for the implementation of the use case in Spain.
- End-to-end accountability assessment of the use case based on [4], that allows to identify specific accountability requirements for the different stages of the system lifecycle, and that will also serve to improve the questionnaire for biometrics.

The different requirements have been grouped by the assessment carried out for their extraction. The following table below explains the identifiers used.

ID	*Source*
*REQ_QUE_**	Extracted from the SALT Questionnaire for biometrics
*REQ_SOC_**	Obtained through the socio-ethical assessment described in section 3.2
*REQ_VSS_**	Extracted from the guide on video surveillance of the AEPD
*REQ_LEG_**	Legal requirements obtained through the assessment explained in section 3.4
*REQ_ACC_**	Accountability requirements obtained through the assessment explained in section 3.4

Table 4: List of IDs for the different requirements

All the concerns and requirements identified are summarized in section 3.5.

3.1 SALT Questionnaire for biometric systems

An initial privacy impact assessment of the system has been done through the first version of the SALT questionnaire developed in this project, that is based on the European data protection legal framework and the ISO privacy framework.

From the questionnaire, it is worth stressing that the most critical aspects to be evaluated before the design stage for biometric systems are the **proportionality** and **legitimacy** of the system. The European Data Protection Directive 95/46/EC states that biometric data (and other kind of personal data) may be collected and processed only under a limited and exhaustive list of circumstances that delineate the legitimate grounds for the processing of personal data. In

this case, Visual Tools invokes its "legitimate interests", in particular the protection of its property, therefore it is necessary to ensure that there is no other less intrusive solution that could be used to solve the stakeholder problems. For this, it is required to make an in-depth study of the problems to be solved, and also of other approaches, technological and non-technological, to justify that the use of the biometric system is necessary and that it is undoubtedly the best solution.

The technology or technologies selected must be carefully evaluated too. On the one hand it is important to determine the **intrusiveness of the technology**. Not all the biometric technologies have the same impact on the different types of privacy, and it is necessary to identify all the possible data protection risks associated to the use of the selected technology, in order to evaluate if the risks are proportionate in relation to the defined purpose. In the case of bodyprints, they are clearly less intrusive than other biometric solutions that identify unequivocally a person under any circumstances (e.g. face, DNA, fingerprint), and more respectful with privacy than other non-biometric approaches that require the collection of more personal information.

On the other hand, a bad **performance of the system** may cause that an authorized person is considered unauthorized, and his/her privacy can be compromised because of this error. The bodyprints have produced very good results for the recognition of people wearing uniforms in the tests carried out under conditions similar to the scenario where the system will be deployed. Anyway, specific measures will be implemented to mitigate the consequences of a possible error in the matching process (e.g. human verification of results required).

The questionnaire also includes several questions about the technical implementation of the system, in order to identify the risks associated to the collection and treatment of personal data with the procedures defined, such as the involvement of data subjects during the processes of enrolment and matching to ensure **transparency**. As the biometric system proposed does not require the collaboration of individuals during the matching phase, it is necessary to implement additional mechanisms to inform any data subject appearing in the office about the surveillance activities being carried out.

Besides, the different **design decisions** that can be made provide different levels of risks regarding privacy. The most critical design choice for this system, is the use of a centralized database for the storage of biometric templates, which should be avoided according to the recommendations of the Working Party. In this case it is strictly necessary to use a centralized storage to identify authorized people with the selected technology in the scenario described, thus it is required to implement sufficient security measures to compensate the use of this type of storage and protect adequately the biometric templates.

Moreover, the **protection against identity theft** is crucial in systems used for identification, therefore particular attention should be paid to the anti-spoofing mechanisms to be implemented, identifying any possible cause of identity manipulation or theft, and providing for each a solution to avoid it or mitigate its consequences.

The complete list of requirements extracted from this questionnaire is shown in section 3.5 *(REQ_QUE_*)*.

The final version of the questionnaire will be fully described in deliverable D2.4, and the version used for the evaluation of this use case is enclosed to this deliverable *(*Appendix A: SALT questionnaire for biometrics*)*.

3.2 Additional socio-ethical requirements

In every enrolment phase, it is crucial to explain pedagogically the objectives of the surveillance system (cf. duty to inform), as well as to guarantee that his/her privacy will be respected, and how it will be. It is not possible, due to the specific context of this use-case, to require an informed consent; but it is desirable to have this phase of didactic information and explanation *(REQ_SOC_1)*.

We know that the main part of the cleaning employees are women, often of foreign origin and/or with very low qualifications. These background characteristics must be taken into consideration. Indeed, women are more prone to bodily changes such as pregnancy, or gaining or losing weight. How does the system react to these changes? It is important to foresee the possibility of such changes without creating a crisis or triggering an alarm, which have an impact on the social relationship between workers *(REQ_SOC_2)*. It is thus important to be careful with the stigmatization of workers, who then will risk reinforcing an anticipative conformism already at work in every situation of monitoring and surveillance. In addition, the cleaning sector is often subject to a large turnover. It often has temporary staff or trainees. It is also interesting to anticipate these frequent changes in staffs.

A proactive answer to this could be an update of the bodyprints every 6 months, or more frequently, a on demand of the maintenance employees. Besides, the system monitors the accuracy of the bodyprints to detect outdated biometric templates.

Sensitive issues resides thus in the ability of the biometrical system to manage change *(REQ_SOC_3)*. For example, what will happen if one of the staff's employee forgets his uniform? If the system is too sensitive (false alarm) and too closed, it may appear intrusive to employees and ineffective for SA and SO.

This use-case shows a quite non-intrusive biometric system, like the Facial Recognition System. As Introna and Wood (2004: 183) underlined [1], Facial Recognition System as a biometric system can be designated as a *silent technology*, in opposition to *salient technology:*

***Silent* technology is:**	***Salient* technology is:**
Embedded / hidden	On the 'surface' /conspicuous
Passive operation (limited user involvement)	Active operation (fair user involvement)
Application flexibility (open ended)	Application stability (firm)
Obscure (form/operation/outcome)	Transparent (form/operation/outcome)
Mobile (*soft*-ware)	Located (*hard*-ware)

Table 5: Silent versus Salient Technology

Facial recognition algorithms in 'smart' CCTV is a particularly good example of a silent technology. The facial recognition capability can be imbedded into existing CCTV networks, making its operation impossible to detect. Furthermore, it is entirely passive in its operation. It requires no participation or consent from its targets—it is "non-intrusive, contact-free process".

The body prints system can be also considered as a silent technology. It means that even if the intrusive impacts seem limited, they exist but remain invisible. In order to alleviate these impacts, an intermediate neutral space, not monitored, could be provided *(REQ_SOC_4)*. This space would be located between outside and the Visual Tool areas, in order to provide "surveillance breaks" .

In addition, while night work is more precarious for workers – especially women, we can imagine that this space could serve as a waiting room for outsiders, without triggering the alarm system *(REQ_SOC_5)*.

3.3 National legislation

As the biometric system described in the previous section is going to be deployed in Spain, it has to comply with the Spanish legislation.

In Spain, the biometric data are considered personal data and therefore their treatment is regulated by the Organic Law 15/1999 on the Protection of Personal Data (LOPD) [2], that is consistent with most of the contents of the Directive 95/46/EC.

The main concerns and requirements extracted from the LOPD are already covered by the questionnaire for biometrics developed in this project, and summarized in section 3.1, such as the principles of quality, proportionality and purpose of the processing.

The Spanish Data Protection Agency has also developed a guide on video surveillance, which tries to provide practical criteria and directions to ensure appropriate compliance with the current Spanish legislation in all cases [3]. As the proposed biometric system uses video cameras to collect the biometric data, the recommendations of this guide shall be applied, among which the following are noteworthy [3]:

- **Duty to inform (REQ_VSS_1-2):**

" Providing the proper information on any data collection procedure is a key element in the right to data protection and compliance with this requirement is therefore obligatory. However, the special characteristics involved in video surveillance call for the design of specific procedures to inform persons whose images are being captured.

Instruction 1/2006 includes an informative sign whose use and display is mandatory. The sign will be placed at least in the entrances leading onto the areas under surveillance, whether these be indoors or outdoors. If the site under surveillance has many entrances, the sign must be fitted in all of them so that the information may be seen regardless of the entrance used.

The file controller must also make available a printed handout with all the information laid down in Article 5 LOPD. This handout will, hence, include information at least on the following:

- *The existence of a personal data file or processing arrangement, the purpose behind collecting the data and the recipients of the said the information.*
- *The possibility of exercising the rights to data access, rectification, cancellation and objection.*
- *The identity and address of the data processing controller or, as the case may be, the representative.*

The handout will have to be available, or at least there must be the possibility of printing it, upon request from the data subject. The information on the handout may also be included on the informative sign, and this sign may replace the handout only in those cases in which its content and location make the information legible and intelligible."

- **Inscription of the system in the General Register (REQ_VSS_3):**

  " If the video surveillance system generates a file, the controller must notify the Spanish Data Protection Agency beforehand, and register the said system with the Agency's General Register. This shall take place whenever there is any type of recording."

- **Position of the cameras (REQ_VSS_4):**

  " Cameras and video cameras set up in private areas shall not obtain images from public areas.

  Partial and limited images of public thoroughfares may be taken when this is essential for the surveillance purpose in view or it is impossible to avoid doing so because of the location of the cameras.

  In any case the use of video surveillance system shall always respect personal rights and abide by the rest of the legal system. E.g. It would not be permissible to capture images in spaces protected by the right to privacy, such as the interiors of nearby dwellings, in bathrooms or dressing rooms or physical spaces outside the sphere specifically protected by the surveillance system."

- **Retention period for the images stored (REQ_VSS_5):**

" Article 6 of Instruction 1/2006 lays down a one month deadline for cancelling images, running from the date when they were captured. This deadline follows the same criterion as that laid down in Article 8 of Act 4/1997 of 4th of August regulating the use of video cameras by National Security Forces in public places.

Once this deadline has been reached, therefore, the images must be cancelled. This means that they must be blocked as laid down in Organic Law 15/1999 and the RDLOPD, whereupon they are kept available only for Public Authorities, Judges and Courts for dealing with any processing liabilities that may arise until the liability time bar lapses. Once the time bar has run its course the data must then be erased.

Should the controller ascertain the recording of an administrative infringement or offence that has to be reported to the corresponding authorities and then duly report it, then the images must be kept available for said authority to check them."

- **Security level of the images stored (REQ_VSS_6):**

  " The facility controller shall take all the technical and organizational measures as may be necessary to ensure security of the images and avoid their unautho firm, therefore, whether it be a company, a residents' association, etc, must comply with the duty of guaranteeing the security of the images in the terms laid down by the LOPD and its development Regulation.

  In general, video surveillance files usually have a basic security level. Nonetheless the file controller must assess the security level at all times, bearing in mind provisions of Article 81 of the Regulation in relation of the contents and purpose of the file."

- **Security obligations of people allowed to access the data (REQ_VSS_7):**

  " The controller shall inform people allowed to access the data about their security obligations and secrecy duty under the terms of Article 8 of Instruction 1/2006.

  Furthermore, any person who has access to the data in the performance of his or her duties, will have to maintain due secrecy and confidentiality in relation to the aforementioned data. The controller shall inform the people accessing the data of the secrecy duty [...]."

3.4 End-to-End Accountability for the Biometric Case Study

End-to-end accountability

End-to-end accountability covers the whose data management life cycle, from collection to deletion. We have also included the phase prior to the collection of the data, during which the opportunity of the system is assessed (intention phase), in accordance with the PARIS process. When biometrics are used, we have identified the following phases of the data lifecycle management:

- Intention phase
- data collection (enrolment or registration and matching),
- data storage

- data sharing
- Deletion

Accountability requirements

As described in the Deliverable 2.3, each phase of the data management lifecycle can call for three kinds of accountability mechanisms: policies, procedures and examples of good practices. This obligation is present in article 22 of the proposed General Data Protection Regulation (not approved yet at the moment of writing). According to this article, the controller shall adopt appropriate policies and implement appropriate and demonstrable technical and organizational measures to ensure and be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with the data protection framework. In order to comply with this obligation, it is recommended to develop an internal privacy policy (Privacy Management Program) that will cover the whole data life management cycle. The data controller is required to document and communicate in an appropriate way all privacy related policies, procedures and practices (REQ_ACC_1).

Policies: Should be documented and at minimum include information about the following items:

- collection, use and disclosure of personal information, including requirements for consent and notification;
- procedure to access to and correction of personal information;
- retention and disposal of personal information;
- identify a responsible person for the processing of personal data, technical and organizational measures including administrative, physical and technological security controls and appropriate access controls to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

Procedures: Include organizational measures that have been implemented by the entity in order to ensure that policies are implemented in practice. The data controller could choose and go beyond the minimum requirements for the privacy management program and foresee disciplinary sanctions in case of contravention of the internal policy and procedures, setting up special education programmes for employees and subcontractors, or identify situations under which a Privacy Impact Assessment (PIA) should be conducted.

Practices: the DC should implement the relevant technical measures to ensure that the policies and procedures are implemented 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. In addition, the DC should keep the documentation of the privacy management program and its practices (ISO/IEC 29100; General Data Protection Regulation, Article 28.1). Keeping the documentation could ease internal and external auditing processes. It could also ease the demonstration of DC compliance with the regulatory framework. Following this practice, the DC should also document the PIA process

and its outcomes. The DC should document consultation notice, input received from stakeholders and decision making process.

Data controller, data subjects and data processed in the use case

As defined in section 2.4, the Data Controller (DC) is the company that define the means and purposes of the biometric system. In our case, Visual Tools qualifies as data controller.

The personal data generated by the system are: videos, frames and bodyprints recorded and stored by the surveillance system, and any additional data related to a specific person (such as any metadata, and log information, etc.).

It should be noted that, Data Subjects (DS) are not only individuals whose images have been recorded by the video system, but also individuals who may be captured by the surveillance system during the matching phase. This led us to include under the data collection phase both the enrolment and the matching phases.

We assume that the data controller has already an internal privacy policy in place *(Privacy Management Program)*. Recommendations will point to specific elements that should be added to the Privacy Management Program to cover this new data processing activity.

3.4.1 Intention phase

The intention phase takes place before the actual set up of the surveillance system. Below, the main requirements associated to this phase are described (REQ).

REQ. Perform a Data Protection Impact Assessment (DPIA)

The questionnaire guides the user of the SALT framework throughout a typical DPIA for biometric systems. The output could be integrated in a PIA. The questionnaire can either support the user in conducting the DPIA or allows the user to check whether all aspects were taken into account.

Legal requirement (REQ_LEG_1): The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks. (General Data Protection Regulation, Article 32a). The controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subjects, especially their right to protection of personal data. The General Data Protection Regulation defines cases where conducting a DPIA is mandatory and its minimum content.

It is mandatory in the following cases:

- processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;
- processing of sensitive data, location data or data on children or employees in large scale filing systems;
- profiling on which measures are based that produce legal effects concerning the

individual or similarly significantly affect the individual;

- processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
- automated monitoring of publicly accessible areas on a large scale;
- other processing operations for which the consultation of the data protection officer or supervisory authority is required
- where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;
- 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;
- where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.

The assessment should have regard to the entire lifecycle management of personal data from collection to processing to deletion and contain at least:

- a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation;
- a description of the measures envisaged to address the risks and minimise the volume of personal data which is processed;
- a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned;
- a general indication of the time limits for erasure of the different categories of data;
- an explanation which data protection by design and default practices have been implemented;
- a list of the recipients or categories of recipients of the personal data;
- where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article44(1), the documentation of appropriate safeguards;

Accountability requirements:

Policies (REQ_ACC_2): The Privacy Management Program should indicate when a DPIA should

be performed, the process to be followed, the persons to be involved in the process (such as the Data Protection officer) and the minimum content of the PIA.

Procedures (REQ_ACC_3): Although the DPIA is conducted prior to setting up a surveillance system, it is not a one-time measure – it should be reviewed on a regular basis. In cases where a DPIA indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects (e.g., exclude individuals from their right, or by the use of specific new technologies), the DC is recommended to consult relevant supervisory authority (General Data Protection Regulation, Article 34.2.a).

Practice (REQ_ACC_4): The DC should keep the documentation of the Privacy Management Program and its practices (ISO/IEC 29100; General Data Protection Regulation, Article 28.1). Keeping the documentation could ease internal and external auditing processes. It could also ease the demonstration of DC compliance with the regulatory framework. Following this practice, the DC should also document the DPIA process and its outcomes. The DC should document consultation notice, input received from stakeholders and decision making process.

REQ. Consultation of stakeholders

Legal requirement (REQ_LEG_2): Consultations of data subjects is mandatory in the context of Data Protection Impact Assessments. Article 33.4 GDPR 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*".The DC should inform stakeholders about the outcome of the DPIA exercise. In order to comply with this obligation, the DC should follow a three steps process: (1) identify affected data subjects (we recommend to involve all stakeholders affected by the implementation of the system, not only data subjects), (2) Define and enable channels of participation, (3) Inform about the outcome of the decision.

The goal is to understand the different expectations people affected by the implementation of the surveillance system might have towards the new system to be put in place and take these concerns into account in the decision to design and deploy the surveillance system. The goal of the consultation is twofold: (1) to explain the purpose, rationale and envisaged modalities of the system, and (2) gather the views of stakeholders with regard to the impact such system might have on their work.

Accountability requirements:

Policies (REQ_ACC_5): the privacy management program should describe how to identify stakeholders and potential consultation processes and the need to draft a report at the end of the consultation phase explaining how the system integrates the concerns raised and the reasons why certain concerns were not taken into account.

In this case study, stakeholders affected by the implementation of the system are: VT employees, maintenance company employees, security company.

Procedures (REQ_ACC_6): Implement adequate procedures for the consultation of

stakeholders.

In the case study, adequate channels of participation are:

- Staff meeting with VT employees: the use of the news system has a minimum impact on VT employees. They are informed of a new procedure to access the building at night.
- Bilateral consultation with the maintenance company: employees of the company feel threatened by the fact that their bodies will be scanned. VT explain to them that the system will be designed to reduce the impact on their privacy: bodyprints are stored in a secure way, only the template is stored, the data is not used for any other purpose.
- Bilateral consultations with the security company: at that stage, the security company is not impacted as the use of the system will only reduce the number of alerts they receive. It has no impact on the existing procedure.

Practices (REQ_ACC_7): Draft a report at the end of the consultation phase explaining how the system integrates the concerns raised and the reasons why certain concerns were not taken into account.

3.4.2 Collection phase

Collection of personal data happens at two different phases:

(1) *Enrolment*: capture of bodyprints of employees authorized to access the premises of VT at night
(2) *Matching*: capture of bodyprints of authorized and non authorized persons

3.4.2.1 Enrolment phase

The enrolment phase is at the core of the biometric system. During this phase biometric data of a particular data subject is captured and aligned with an identity. Typically, the enrolment is performed offline by the System Administrator (SA) who is authorized by the DC to record a video using one of the VPUs. This video is captured from one of the depth cameras with a specific user interface available in the VPUs. Later, the bodyprint is extracted from the video sequence.

REQ. General accountability requirements for the enrolment phase

Policies:

- (REQ_ACC_8) Define the procedure to assign responsible personnel for the enrolment phase.
- (REQ_ACC_9) Define the enrolment procedure (instructions to the personnel).
- (REQ_ACC_10) Defined circumstances under which the enrolment procedure has to be repeated (e.g., on periodic basis every 6 months, after false alerts, and etc.).
- (REQ_ACC_11) Ensure that responsible personnel has received adequate privacy and security awareness training to perform enrolment.

- (REQ_ACC_12) Ensure that only authorization of personnel carries out enrolment into the system.

Procedures:

- (REQ_ACC_13) Assign responsible personnel for the enrolment phase
- (REQ_ACC_14) Provide responsible personnel with instructions of the enrolment procedure.
- (REQ_ACC_15) Provide responsible personnel with adequate privacy and security training.
- (REQ_ACC_16) Ensure that only authorized personnel carries out enrolment into the system

Practices:

- (REQ_ACC_17) Trace data collection processes during the enrolment (records or logs).

REQ. Transparency of the enrolment process *(REQ_QUE_5)*

Legal requirement (REQ_LEG_3): Data subject must be informed of the data processing activity before their data are collected. The information provided to the data subject of the controller should include the following information that would be provided to the data subject at the enrolment stage:

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

Accountability requirements:

Policy (REQ_ACC_18): The policy should indicate that when personal data are collected directly from data subjects, the information should be provided before the time of collection (before the enrolment). It should specify the content of information notice when video surveillance cameras are installed. The information notice that is communicated to data subject during the enrolment phase should contain the following items:

- a description or visualization of the matching procedure during which extracted bodyprints allow to identify a person (Biometrics Constitution).
- Explanation of how data subject's rights (access, rectification, and erasure) can be exercised in this phase.
- Explain a repudiation procedure during which an identified person could provide evidence proving the wrong identification of the matching phase.

Procedure (REQ_ACC_19): The policy should indicate how the information should be handed in to data subjects (on paper, orally, information notices placed on visible area close to the cameras, etc.).

Practice (REQ_ACC_20): Keep evidences that the data subject has been provided with the information notice prior to the enrolment into the system.

REQ. Data minimization

Legal requirement (REQ_LEG_4): The collected personal data should be strictly limited to the necessary data to meet the purposes that have been provided in the information notice.

Accountability requirement:

Policy (REQ_ACC_21): The internal policy clearly states the purposes of collection and define accordingly which information is necessary to meet this purpose.

Practice (REQ_ACC_22): The system is designed to allow the recording only of the data necessary to achieve the purposes of the data processing activity.

3.4.2.2 Matching

It is the process of comparing biometric data/template (captured during enrolment) to the biometric data/template collected from a new sample for the purpose of identification, verification/authentication or categorisation. Biometric systems use two or more biometric traits/ modalities from the same individual in the matching process. These systems can work in different ways, either collecting different biometrics with different sensors or by collecting multiple units of the same biometric. (WP 193 Opinion 3/2012 on developments in biometric technologies).

In this use case, during the matching phase the system performs the recognition of people to check if they are authorized or not to access the office. The VPUs during this phase are continuously analysing the images from the depth cameras in order to detect the people

appearing in the scene and to extract their bodyprints. In this case the data subjects are not only persons enrolled into the system but all the individuals who may appear in the areas subjected to video surveillance. In case of non-authorized persons, the data collection accountability measures can be a bit different from the case of authorized people. During the matching phase, the RIS compares any new collected bodyprint with the APDB. Once compared, the bodyprints are removed from the system, and the results of the matching process are temporary stored in the RIS and the RMS until they are validated by the SO.

REQ. General accountability requirement for the matching phase.

Policies (REQ_ACC_23): It is recommended that internal and external data management policies cover the procedures and practices of data processing, including the matching phase:

- Describes or visualizes the procedure during which extracted bodyprints allow to identify a person (Biometrics Constitution).
- Foresees organizational and technical measures that would address risks associated with the data processing (e.g., adjust position of cameras, that only necessary data is collected to perform matching).
- Specifies policies and procedures for positive and negative matching outcomes. (REQ_QUE_9)
- Requires that the DC has responsibility to inform authorized personnel about policies and procedures for positive and negative matching outcomes.

Procedures:

- (REQ_ACC_24) Include organizational measures that have been implemented by the entity in order to ensure that policies are implemented in practice.
- (REQ_ACC_25) Describe or visualize the procedure during which extracted bodyprints allow to identify a person (Biometrics Constitution).
- (REQ_ACC_26) Foresees organizational and technical measures that would address risks associated with the data processing (e.g. adjust position of cameras, that only necessary data is collected to perform matching).
- (REQ_ACC_27) Follow special policies and procedures for positive and negative matching outcomes. *(REQ_QUE_9)*
- (REQ_ACC_28) DC has to inform authorized personnel about policies and procedures for positive and negative matching outcomes.
- (REQ_ACC_29) Ensure that there are policies and procedures in place that ensure that data subject's rights can be exercised.
- (REQ_ACC_30) Provide a separate notification in the area where surveillance system collects additional data to perform matching.
- (REQ_ACC_31) DC has to audit is data management practices.

Practices:

- (REQ_ACC_32) Trace all data collection processes during the matching phase (e.g. system logs, log analyzer);
- (REQ_ACC_33) Informal obligations to be verified;

REQ. Transparency of the matching process *(REQ_QUE_6)*

Legal requirement (REQ_LEG_5): As it is the case during the enrolment phase, the active participation of the individual during the matching phase, whenever possible, constitutes a preferable option since it is a good opportunity for him/her to be aware of the processing of his/her biometric data. At least, data subjects must be informed of the data processing activity before their data are collected.

Accountability requirements:

Practice (REQ_ACC_34): A separate notification should be provided in the area where surveillance system collects additional data to perform matching. For example, a board on the wall informs about the surveillance activities.

3.4.3 Data Storage

The data obtained during enrolment can be stored locally in the operations centre where the enrolment took place (e.g. in a reader) for later use, or on a device carried by the individual (e.g. on a smart card) or could be sent and stored in a centralised database accessible by one or more biometric systems. Taking into consideration the growing standardisation of biometric technologies for interoperability, it is generally accepted that the centralised storage of biometric data increases both the risk of the use of biometric data as a key to interconnect multiple databases (which might lead to creating detailed profiles of an individual) and the specific dangers of the reuse of such data for incompatible purposes especially in the case of unauthorised access (WP 193 Opinion 3/2012 on developments in biometric technologies).

During the enrolment phase in this use case, a video of the authorized person is recorded and stored in one of the VPUs. Later that video is analyzed and a set of bodyprints are extracted, from which the best candidate is chosen. After this process, the video is deleted, and the selected bodyprint is copied by the System Administrator to the *Authorized People Database* (APDB) located in the RIS.

The key frames (images) are obtained in the VPUs for each person detected and sent to the RIS with the corresponding bodyprints. Once sent to the RIS, they are removed from the VPU. After the matching, the RIS copies them with the results of the comparison to the RDB, and they are kept until the alarms are verified by the SO and, in case of intrusion, by the local authorities.

REQ. Security *(REQ_QUE_13)*

Legal requirement (REQ_LEG_6): Adequate measures should be adopted to safeguard the data stored and processed by the biometric system: biometric information must always be stored in an encrypted form.

Accountability requirement:

Policies (REQ_ACC_35): The internal privacy policy (internal privacy management program) of the controller could include information concerning data management procedures, such as :

- Defined organizational and technical procedures ensuring security of recorded videos. This would include a robust access control system, strong authorization and incident reporting schemes, auditing and periodic review of the need to store information.
- Defined organizational and technical procedures ensuring that only authorized personnel has access to the system into the system.

Practice (REQ_ACC_36): Implement adequate security measures, and document them precisely. Examples:

- Security can be provided by a well-defined access control system and strong authorization scheme.
- Maintain access control logs and review reports should be maintained as the evidence that the access control and security mechanisms are properly implemented, and only authorized members can access the videos and bodyprints.

REQ. Data quality

Legal requirement (REQ_LEG_7): The biometric data should not be kept for longer than necessary to achieve the stated purpose. Each data retention period should be adapted to each category of data.

Accountability requirement:

Policies

- (REQ_ACC_37) Procedures are defined for the periodic review of the accuracy and quality of the bodyprints stored in the Authorized People Database (APDB) located in the RIS, as well as for any additional personal data.
- (REQ_ACC_38) Policies should define data retention period for each category of data

Practices:

- (REQ_ACC_39) Mechanisms are required for the periodic review of the accuracy and quality of the bodyprints stored in the Authorized People Database (APDB) located in the RIS, as well as for any additional personal data.
- (REQ_ACC_40) The recorded videos/frames and bodyprints must carry retention period limits and be kept to a strict minimum.
- (REQ_ACC_41) Implement mechanisms to make sure that retention limits are respected (e.g. logs of data erasure).

REQ. Data subject rights (access, rectification, deletion)

Legal requirement (REQ_LEG_8): Data subjects have the right to access, rectify and request deletion of their personal data

Accountability requirements:

Policy (REQ_ACC_42): Define organisational and technical procedures allowing to answer requests of access and deletion from data subjects, as well as criteria to be used to base rejection of such request

Procedure:

- (REQ_ACC_43) Ensure that data subjects' requests are given proper answers.
- (REQ_ACC_44) Ensure that the procedure to access data is friendly for data subjects

Practice (REQ_ACC_45): Adequate mechanisms shall be implemented to ensure that the rights of data subjects over their personal data (access, rectification, deletion) are respected. Some examples of this type of mechanisms are:

- Provide samples of data subject interaction for access/rectification/deletion
- Use a secured web page for data rectification request
- Log of messages to data subjects ensuring updated data
- Log analysis

3.4.4 Sharing

Data sharing occurs when access to the system is required by third parties who are not acting on behalf of the controller.

REQ. Limitation of the access to personal data *(REQ_QUE_10)*

Accountability requirements mandate that the DC should check that these access are based on legal bases and recorded by the system.

Policies (REQ_ACC_46): The procedure to analyze the validity of a request and to give access to the system should be defined.

Procedure (REQ_ACC_47): Mechanisms in place shall be implemented to trace the access given to the system.

Practices:

- (REQ_ACC_48) The person in charge of receiving and transmitting the request should document the request the controller receives from a third party, any decisions undertaken in relation to this request. The Data Protection Officer should include his name and contact details in documents he is issuing (The proposed General Data Protection Regulation; Article 28.2(b)).
- (REQ_ACC_49) Actions undertaken in a response to a formal request from the competent authority to provide access to relevant data should be documented.
- (REQ_ACC_50) Access to the data contained in the system should be traced:

- person who accesses,
- basis for access,
- purpose of access,
- data accessed/modified/deleted/extracted (collection, alteration, consultation, disclosure, combination or erasure).[1]

3.4.5 Deletion

REQ. Retention and deletion of personal data *(REQ_QUE_14)*

Legal requirement (REQ_LEG_9): In order to prevent that biometric information are stored for longer than is necessary for the purposes for which they were collected or subsequently processed, appropriate automated data erasure mechanisms have to be implemented also in case the retention period may be lawfully extended, assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system. (WP 193 Opinion on Biometrics).

Accountability requirements:

Policy (REQ_ACC_51): Definition of internal and external data management policies that cover procedures and practices of data processing, including:

- organizational and technical measures that would address risks associated with the data processing deletion phase;
- organizational and technical measures that would allow to trace actions undertaken in the deletion phase;
- data retention periods and that collected personal data is not kept longer as necessary for the purposes of the system.

Procedures: DC is required to perform the following actions:

- (REQ_ACC_52) Implement organizational and technical measures that would address risks associated with the data processing deletion phase.
- (REQ_ACC_53) Ensure that data retention periods are adhered to and that collected personal data is not kept longer as necessary for the purposes of the system.

[1] There is no specific obligation under the proposed General data protection regulation but we can take as example the Law Enforcement Data Protection Directive which will mandate law enforcement authorities to keep records of at least the following personal data processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show in particular the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such data. The records shall be used solely for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security, or for the purposes of auditing either by the data protection officer or by the data protection authority.

Practice (REQ_ACC_54): Mechanisms should be implemented to ensure that the data deletion processes work as expected (e.g. use of logs to record data erasure processes, use of a log analyzer).

3.5 Summary of privacy and accountability concerns

This summary contains requirements extracted from the following sources:

- The draft SALT questionnaire for biometrics (REQ_QUE_*). The main topics covered by the questionnaire have been turned into requirements for the system.
- The socio-ethical assessment described in section 3.2.
- The Spanish DPA's guideline for video surveillance systems, based on the Spanish legislation (REQ_VSS_*).
- The evaluation of the system in terms of accountability explained in section 3.4 (only the concerns not covered by other requirements in the table are shown in this section).

ID	Requirement	Related Req.	Artifacts
[QUE]	*EXTRACTED FROM THE QUESTIONNAIRE*		
REQ_QUE_1	**Purpose** Define clearly the **purpose** of the processing of personal data, for which the evaluation of the stakeholder's problems is required.	*REQ_LEG_1, REQ_ACC_1* *(Shall be indicated in the DPIA report & the PMP)*	**A1, A2, A21**
REQ_QUE_2	**Legitimacy** Indicate and justify the **legal ground** on which the implementation of the biometric system relies.	*REQ_LEG_1, REQ_ACC_1* *(Shall be indicated in the DPIA report & the PMP)*	**A1, A2**
REQ_QUE_3	**Proportionality** Justify the **necessity and suitability** of the system and the selected technologies for the defined purpose.	*REQ_LEG_1, REQ_ACC_1* *(Shall be indicated in the DPIA report & the PMP)*	**A1, A2, A22**
REQ_QUE_4	**Interference with privacy rights** Data protection risk assessment, identifying the potential impacts on individual's rights.	*REQ_LEG_1, REQ_ACC_1* *(Shall be indicated in the DPIA report)*	**A1**
REQ_QUE_5	**Transparency of the enrolment process** *Enrolment of people without their knowledge and/or consent, implying a covert collection, storage and processing of biometric data is as a principle, excluded.*	*REQ_VSS_2, REQ_LEG_3, REQ_ACC_8-20* *(and any other requirement related to the data processing during the matching phase and the duty to inform; shall be indicated in the PMP)*	**A2, A5**

REQ_QUE_6	**Transparency of the matching process** *As it is the case during the enrolment phase, the active participation of the individual during the matching phase, whenever possible, constitutes a preferable option since it is a good opportunity for him/her to be aware of the processing of his/her biometric data.*	*REQ_VSS_1-2, REQ_LEG_5, REQ_ACC_23-34* *(and any other requirement related to the data processing during the enrolment phase and the duty to inform; shall be indicated in the PMP)*	**A2, A4**
REQ_QUE_7	**Privacy impact of the technology selected** Description of the technology selected and its impact on privacy taking into account the type of matching performed.	*REQ_LEG_1, REQ_SOC_3-4 REQ_ACC_2-4* *(Shall be indicated in the DPIA report)*	**A1**
REQ_QUE_8	**Nature of the data collected** Description of the biometric data collected, and also of any other category of personal data, during the enrolment and matching, including the purposes of its collection and the target groups affected.	*REQ_LEG_1, REQ_ACC_1* *(Shall be indicated in the system documentation - PMP)*	**A1, A2, A11**
REQ_QUE_9	**Expected system accuracy** Impact on privacy of the expected system accuracy and the errors that may occur (e.g. false positives and false negatives).	*REQ_ACC_46-50* *(Shall be explained in the system documentation, and taken into account in the DPIA)*	**A1, A11, A15, A18**
REQ_QUE_10	**Limitation of the access to personal data** Description of the different users that can have access to the personal data stored in the system and justification of that access.	*REQ_ACC_46-50, REQ_VSS_7* *(Shall be indicated in the system documentation)*	**A6, A7, A9, A11, A20, A21**
REQ_QUE_11	**Disclosure of personal data** Description of the circumstances in which the data can be transferred to third parties (if any).	*REQ_ACC_1, REQ_ACC_46* *(Shall be indicated in the system documentation - PMP)*	**A1, A2, A11, A24**
REQ_QUE_12	**Storage of personal data** *Whenever it is permitted to process biometric data, it is preferred to avoid the centralized storage of the personal biometric information.*	*REQ_ACC_1* *(Shall be indicated in the system documentation)*	**A11**
REQ_QUE_13	**Security of the data stored** *The biometric data and any other personal data collected and stored by the system should be properly protected. In addition, the biometric templates should be also*	*REQ_LEG_6, REQ_ACC_35-36, REQ_VSS_6* *(Shall be described in the system documentation)*	**A6, A11, A12, A13, A14, A20, A21**

	protected if there is any possibility of misuse or of retrieval of the data source.		
REQ_QUE_14	**Retention and deletion of personal data** *The retention duration of biometric data, and also of any other personal data, should be assessed carefully. The data shall not be kept for longer than is necessary to achieve the stated purpose(s). This implies that once the data is not necessary anymore, it should be immediately deleted/erased. Also, each retention duration should be adapted to each category of data.*	*REQ_ACC_51-54, REQ_LEG_7, REQ_LEG_9, REQ_VSS_5* *(and any other requirement related to data quality; shall be explained in the system documentation - PMP)*	**A1, A2, A5, A10, A11**
REQ_QUE_15	**Protection of personal data communications** Data transmissions should be adequately protected, to avoid unwanted disclosure of personal information.	*REQ_LEG_6* *(Shall be described in the system documentation)*	**A11, A12, A13, A20**
REQ_QUE_16	**Privacy impact of system failures** The impact on privacy of a failure in the system components must be evaluated.	*REQ_SOC_5* *(Shall be considered in the DPIA, and included in the system documentation - PMP)*	**A1, A16**
REQ_QUE_17	**Control of unattended operations** It is also important to identify the operations performed without any user interaction, and to implement the adequate mechanisms to control them in order to verify that they are working as expected.	**Any requirement related to the transparency of system processes, e.g. REQ_LEG_4, REQ_ACC_22* *(Shall be described in the system documentation - PMP)*	**A8, A10, A11, A15, A16**
REQ_QUE_18	**Stability of biometric templates** Evaluation of the stability of templates in time, and definition of mechanisms and procedures for their renewal or update in case it is necessary.	*REQ_LEG_7-8, REQ_ACC_37, REQ_ACC_39, REQ_ACC_42-45, REQ_SOC_2* *(Shall be described in the system documentation - PMP)*	**A5, A11, A15, A18, A19**
REQ_QUE_19	**Anti-spoofing measures** *To maintain the reliability of a biometric system and prevent identity fraud the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person. In respect of facial recognition, it may be critical to ensure that the face is a real one and not for example, a*	*REQ_QUE_13, REQ_LEG_6, REQ_VSS_6* *(Shall be described in the system documentation - PMP)*	**A9, A10, A15, A16, A18, A20, A21**

	picture tied on an impostor's head.		
[SOC]	**ADDITIONAL SOCIO-ETHICAL REQUIREMENTS**		
REQ_SOC_1	Didactic explanation of the objectives and functioning of the surveillance system during the enrolment phase.	*REQ_ACC_1* *(a report shall be generated)*	**A25**
REQ_SOC_2	Mitigate the social impact of any change in the group of people enrolled in the system (e.g. bodily changes, new employees, etc.).	*REQ_QUE_18*	**A5, A15, A18**
REQ_SOC_3	Mitigate the social impact of the dependence of the system performance on the clothes of the people enrolled in the system (e.g. staff employee forgetting the uniform).	*REQ_QUE_7* *(Shall be described in the system documentation)*	**A15**
REQ_SOC_4	Reduce the intrusive impact of the system on employees due to the use of a silent technology.	*REQ_QUE_7* *(Shall be described in the system documentation - PMP)*	**A26**
REQ_SOC_5	Mitigate the impact on the social behaviour of employees of the installation of a surveillance system (e.g. taking the children of employees to the office).	*REQ_QUE_16* *(Shall be described in the system documentation - PMP)*	**A26**
[VSS]	***ADDITIONAL REQUIREMENTS FOR VIDEO SURVEILLANCE***		
REQ_VSS_1	**Use of informative signs** *An informative sign, whose use and display is mandatory, will be placed at least in the entrances leading onto the areas under surveillance, whether these be indoor or outdoors.*	*REQ_QUE_6, REQ_LEG_5, REQ_ACC_34*	**A4**
REQ_VSS_2	**Use of an informative handout** *The file controller must also make available a printed handout with all the information laid down in Article 5 LOPD.*	** Any requirement related to the duty to inform about the treatment of personal data, e.g. REQ_ACC_1, REQ_QUE_5-6*	**A2**
REQ_VSS_3	**Inscription of the system in the General Register** *If the video surveillance system generates a file, the controller must notify the Spanish Data Protection Agency beforehand, and register the said system with the Agency's*	-	**A3**

	General Register.		
REQ_VSS_4	**Location of the cameras** *Cameras and video cameras set up in private areas shall not obtain images from public areas.*	-	**A23**
REQ_VSS_5	**Retention period for the images stored** *The images will be preserved only for the time required for fulfilling the purpose for which they were captured.*	*REQ_ACC_51-54, REQ_LEG_7, REQ_LEG_9* *(and any other requirement related to the retention of data; shall be explained in the system documentation - PMP)*	**A2, A10, A11**
REQ_VSS_6	**Security level of the images stored** *The facility controller shall take all the technical and organisational measures as may be necessary to ensure security of the images and avoid their unautho firm.*	*REQ_QUE_13, REQ_QUE_19, REQ_LEG_6, REQ_ACC_35-36* *(Shall be described in the system documentation)*	**A6, A11, A12, A13, A14**
REQ_VSS_7	**Security obligations of people allowed to access the data** *The controller shall inform people allowed to access the data about their security obligations and secrecy duty under the terms of Article 8 of Instruction 1/2006.*	*REQ_ACC_1* *(Shall be described in the system documentation - PMP)*	**A7**
[LEG/ACC]	**ADDITIONAL ACCOUNTABILITY REQUIREMENTS**		
REQ_ACC_1	**Documentation and communication of policies, procedures and practices** *The data controller is required to document and communicate in an appropriate way all privacy related policies, procedures and practices, to be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with the data protection framework (internal and external privacy policies).*	*REQ_SOC_1* *(any other requirement related to transparency and the duty to inform)*	**A2, A11, A24, A25**
REQ_LEG_2	**Consultation of stakeholders** *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*	*REQ_ACC_5-7* *(procedures to be described in the PMP)*	**A25**

	operations		
REQ_LEG_8	**Data subject rights (access, rectification, deletion)** *Data subjects have the right to access, rectify and request deletion of their personal data.*	*REQ_QUE_18, REQ_ACC_42-45* *(procedures to be described in the system documentation)*	**A19**

Table 6: Privacy and accountability requirements identified for the use case

4 Artifacts

An artifact in this context is defined as a procedure, mechanism or measure implemented to address any of the concerns identified for the use case. The table below summarizes the artifacts used in the biometrics scenario to address the concerns on privacy and accountability described in the previous section. There are many other measures that can be implemented, the selection of them depend mainly on the preferences of the system designer, and on the business constraints.

ID	Artifacts	Concerns covered
A1	***SALT Framework questionnaire for biometrics*** Analysis through the PIA questionnaire provided by the SALT Framework of the purpose, necessity and legitimacy of the system, and its potential impact on individuals' privacy. A report containing the rationale of each response.	*REQ_QUE_*, REQ_LEG_1, REQ_ACC_2-4* *(and any other requirement related to the evaluation of the privacy impact)*
A2	***Public privacy policy*** Elaboration of a privacy policy, in which the purpose of the system and the treatment of personal data is explained. This policy will be sent to the people to be enrolled in the system as authorized, and also to the employees of the client company working at the office where the system is going to be deployed. It will also be available for any data subject that requests it.	*REQ_QUE_*, REQ_LEG_2, REQ_ACC_4-5, REQ_VSS_2* *(and any other requirement related to the duty to inform)*
A3	***Inscription of the system in the General Register*** Visual Tools keeps a copy of the form provided to the AEPD for the inscription in the Agency's General Register of the video surveillance system installed at the Visual Tools headquarters, and also the favorable resolution for the registration of the system.	*REQ_VSS_3*
A4	***Use of informative signs*** Informative signs will be placed at least at the entrances leading onto the areas under surveillance.	*REQ_QUE_6, REQ_VSS_1, REQ_ACC_34* *(and any other requirement related to the duty to inform during the matching phase)*
A5	***Definition of a procedure for enrolment in which the collaboration of the data subject is required*** In the system documentation, the process for the enrolment of people will be described, and also the periodicity for the revision and renewal of bodyprints (at least once every 6 months).	*REQ_QUE_5, REQ_LEG_3, REQ_ACC_18-19, REQ_ACC_37, REQ_ACC_39, REQ_LEG_7*
A6	***Role-based access control***	*REQ_QUE_10, REQ_QUE_13,*

	The access to the different system resources (interfaces, programs and data stored) will be restricted to certain users, being this roles defined: ● *System Administrator*: main responsible for the system, with access to all the system resources. ● *System Operator*: user with limited access to the information. The operator will only be able to use the interfaces for matching, and to view the results of the recognition process. ● *System Auditor*: user with limited access to the system resources for auditing. This user will have to request authorization to the *System Administrator* indicating for which purpose the access to the system is required. ● *Data subject*: Data subjects (e.g. people enrolled in the system) will be able to request access to their personal information stored. For this, the authorization of the *System Administrator* is required, and the access is limited to the personal data belonging to that person.	*REQ_VSS_6, REQ_LEG_6, REQ_ACC_35-36*
A7	***Training sessions for the different system users*** We will organize at least two different sessions before the operation phase, to educate System Administrators and System Operators in the use of the system and the different procedures defined, informing them about their responsibilities and security obligations. We will keep a summary record signed by all the participants to prove that the sessions have been held.	*REQ_VSS_7, REQ_QUE_10, REQ_ACC_1*
A8	***Data collection logs*** Data collection processes will be recorded in logs. This logs will contain at least this information: · Date and time · Data collected · Purpose of data collection · The system user (if any) involved in the collection of data	*REQ_QUE_17, REQ_LEG_4, REQ_ACC_22* *(and any other requirement related to the limitation of the collection of personal data)*
A9	***Data access logs*** Any access to the data stored in the system will be recorded in logs. This logs will contain at least this information: · Date and time · Data accessed · Purpose of the access · the system user performing the action	*REQ_QUE_10, REQ_QUE_19,* *REQ_ACC_46-50, REQ_VSS_7* *(and any other requirement related to the limitation of the access to personal data)*
A10	***System logs***	*REQ_QUE_14, REQ_QUE_17,*

	Evidence about the operations performed by the system, such as data handling, will be generated in the form of system logs, containing at least this information: · Date and time of the trace · Modifications on the data stored (if any) · Information of the main operations performed by the system · Information of exceptions or errors detected during the operation of the system	*REQ_QUE_19, REQ_LEG_4, REQ_ACC_22, REQ_VSS_5* *(and any other requirement related to the transparency of system processes)*
A11	***System documentation*** The surveillance system developed will be properly documented for internal use. At least, these documents will be elaborated: ▪ Manual explaining the technical implementation of the system (architecture, components, main system operations, available resources, security mechanisms, how to configure and set up the system, system maintenance, etc.). ▪ Privacy Management Program (PMP) describing the policies, procedures and practices of the company with regards to the processing of personal data. This documents can be provided to any data protection officer auditing the system.	*REQ_VSS_2, REQ_ACC_1* *(and any other requirement related to the implementation of measures and procedures for data protection)*
A12	***Data encryption*** The following information will be encrypted: ● Videos captured during the enrollment process ● Key frames kept for the verification of alarms ● Biometric templates stored in the Authorized People Database (APDB) ● Information transferred between the different system components (e.g. from a VPU to the RIS)	*REQ_QUE_13, REQ_QUE_15, REQ_LEG_6, REQ_VSS_6, REQ_ACC_35-36*
A13	***Connection of devices through a Local Area Network (LAN)*** The VPUs will be connected to the RIS through a LAN, and the remote access to the VPUs and the RIS will be disabled, being required to be physically at the office to use a VPU or the RIS.	*REQ_QUE_13, REQ_QUE_15, REQ_LEG_6, REQ_VSS_6*
A14	***Alarm management separated from the matching process*** It is necessary to use a module to read the results of the matching process, and to generate and send the alarms when an unauthorized access is detected. This module requires connection to the Internet, as the operators may be in a remote control centre. Initially, we thought that this module could be integrated in the RIS, but as the RIS contains the template database (APDB), to increase the database security, it is better to put the module in	*REQ_QUE_13, REQ_LEG_6, REQ_VSS_6*

	another device or partition that only has read access to the results of the matching process through the LAN, and that is just responsible for the generation and emission of alarms.	
A15	***Performance monitoring*** To reduce the risks related to errors in the matching process, an automatic process will review the validation of the matching results, calculating the rate of false positives related to each bodyprint stored in the template database. This will serve to detect inaccurate bodyprints.	*REQ_QUE_9, REQ_QUE_17, REQ_QUE_18-19, REQ_SOC_2-3, REQ_LEG_7, REQ_ACC_37, REQ_ACC_39*
A16	***System monitoring*** The different components will be periodically reviewed by the System Administrator to check that the system is working as expected (at least twice a year). Moreover, other mechanisms have been implemented to facilitate the detection of component failures: ● Anytime the RIS requests information from a VPU, and the VPU does not respond, an alarm will be generated and displayed in a monitoring user interface. ● If a camera stop working, the VPU connected to it will not be able to collect any information, and thus it will not be possible to detect people accessing to the office. In this case, the VPU will not respond to any request from the RIS, so an alarm indicating a problem in the VPU will be generated. ● The monitoring user interface will also show the date and time when the RIS was started, and also when it performed the latest comparison. In case the RIS has not provided any data in the past 48 hours, an alarm will be generated and displayed.	*REQ_QUE_16-17*
A17	***Periodic revision of policies and procedures*** At least every two years the different policies and procedures defined will be reviewed. For this task, the person responsible for the review (e.g. the System Administrator) can use the SALT Framework to check if the concerns have changed. A report with the results and updates made will be generated.	*REQ_ACC_1*
A18	***Creation of a record containing the results of the recognition process*** The results of the matching process and the parameters used in the comparison will be stored, for two main reasons: ● To verify the correct functioning of the biometric system for the detection of unauthorized accesses ● To facilitate the collection of evidences in case of	*REQ_QUE_9, REQ_QUE_18-19*

	intrusion The *System Operator* will be responsible for the reviewing the alarms generated, and validating the results, which also serves to mitigate the consequences of errors in the matching process. After the alarms have been validated by the *System Operator*, for false alarms or positive matches only the date and time where a person was detected will be kept. This prevents the profiling of the data subjects enrolled in the system. In case of true alarm, all the information related to the incident is kept to be provided to the local authorities for law enforcement.	
A19	***Procedure to let data subjects access their personal information*** A specific procedure will be defined to let data subjects have access to their personal data stored in the system, for which the supervision and authorization of the *System Administrator* is required. This process will be described in the system documentation.	*REQ_QUE_18, REQ_LEG_8, REQ_ACC_42-45*
A20	***Access control mechanism for the Web Services*** Authentication and authorization will be required to request information to a VPU through its Web Services. This way, we will prevent unauthorized accesses to the bodyprints stored temporary there.	*REQ_QUE_10, REQ_QUE_13, REQ_QUE_15, REQ_QUE_19, REQ_ACC_50, REQ_VSS_7*
A21	***Access control mechanisms for the User Interfaces*** Authentication and authorization will be required to use the applications developed for setting-up the system, capturing images, enrolment and management of the results. Besides, during the login phase, it will also be necessary to indicate the purpose of the use of the application, which will be recorded in a log with the date and time of the login.	*REQ_QUE_10, REQ_QUE_13, REQ_QUE_19, REQ_VSS_6, REQ_LEG_6, REQ_ACC_35-36*
A22	***Periodic revision of the need for the system*** At least once a year, the efficiency of the system will be evaluated in order to verify if the system based on bodyprints is really necessary and useful. A report with the results of the evaluation will be generated.	*REQ_QUE_3, REQ_ACC_35*
A23	***Document signed by the installer*** The installer is the person (or company) responsible for the deployment of the system at the Visual Tools' Headquarters, and the correct positioning of the cameras, that should not obtain images from public areas. We will keep a document signed by the installer indicating the details of the the installation of the system.	*REQ_VSS_4*

A24	***Action plan in case of unauthorized access*** The actions to be performed in case of intrusion will be detailed in the system documentation. The data collected by the system as evidence of the intrusion will only be shared with the local authorities, which will be traced in, for example, a document signed by the police indicating why they require the information. The data shared with the police will be watermarked, whenever possible, to make clear that the data is shared with the authorities for law enforcement.	*REQ_QUE_11, REQ_ACC_1, REQ_ACC_46*
A25	***Didactic sessions for data subjects*** *In order to inform, and take into consideration the points of view of any data subject, at least two didactic sessions will be scheduled:* ▪ *Session with VT employees* ▪ *Session with maintenance employees* ▪ *Session* *As a result of these sessions, a report will be generated.* *Furthermore, the data controller (VT) is committed to organize additional informative sessions on demand of data subjects if necessary, and whenever possible.*	*REQ_SOC_1, REQ_ACC_1, REQ_LEG_2*
A26	***Provision of "surveillance breaks"*** *Neutral spaces, without surveillance, will be provided in areas close to the entrances and far from the critical areas.*	*REQ_SOC_4-5*

Table 7: List of artifacts to be implemented

5 SALT Framework specialized for biometrics

In this section we highlight the elements of the SALT Framework that are most relevant for the design and development of biometric systems.

5.1 Design process for SALT compliant biometric systems

One of the objectives of this project is the definition of a "by-design" process that enables to ensure that a surveillance system takes into account privacy and accountability from the start, without compromising the surveillance service.

The design process for SALT compliant biometric systems initially described in D6.1 has been updated taking into account ISO/IEC TR 24748-1:2010 [5], which is a guide for life cycle management that, for example, do not consider "Testing" an independent stage, as different types of tests can be performed during several stages. Another important concept integrated is the 3-stage process defined in WP2 for the elaboration of the system design, which is depicted in the figure below.

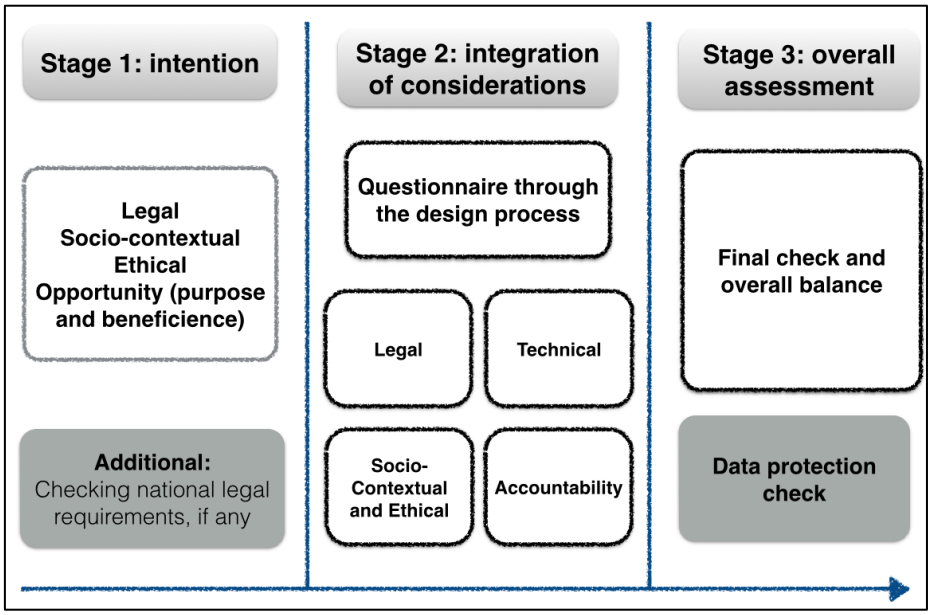

Figure 8: Three stage process for SALT Framework

Stage 1: Intention

The main novelty is the separation of the *Intention stage*, in which the purpose of the system is evaluated, from the collection of other considerations and requirements regarding privacy and accountability. This first stage is specially relevant for biometric systems due to the nature of the data collected and its intrusiveness, which makes biometric technologies inadvisable by the general recommendations on privacy and data protection, unless their use is strictly necessary to achieve a clear and legitimate purpose. Not only it is necessary to justify that there is a necessity to implement the system, but also to ensure that there is no other less intrusive approach that can be used to achieve the goal defined. Thus, as a result of this assessment, a

project based on biometrics can be discarded if it doesn't provide a fair balance of its purposes in terms of proportionality and beneficence.

Once the purpose of the system has been proved to rely on a robust legitimate ground, national legislations should be reviewed in order to identify any legal requirement applicable to the proposed surveillance system. If any, these should be considered high priority requirements.

For this initial assessment, the SALT Framework provides questionnaires that allow to identify the most relevant aspects of the system to take into consideration for an adequate evaluation of its proportionality, and also references to the national legislations to be applied (if any).

This preliminary evaluation requires the consideration of all functional aspects of the system, thus the person or team responsible for this task should have some technical background related to the technologies to be used, apart from legal background on privacy and data protection, having the role of what we define as *System Proposer*.

Stage 2: Integration of considerations

The second stage refers to the collection of requirements for the system, covering legal, socio-ethical, technical and accountability aspects, and their integration in the system design, for which an in-depth revision of how the system will be implemented and used is required.

The SALT Framework provides for this task another set of questionnaires, based on European standards, aimed at assisting designers in the elaboration of a system design for the provision of a surveillance service that solves the stakeholder problems addressing the most relevant concerns on privacy and accountability.

In this case, the target audience of these questionnaires are the *System Proposers*, who should have in mind at least an idea of how the system can be implemented, and the *System Designers*, who are directly responsible for the different design choices and should be aware of the impact on privacy of each of them. In order to understand better the different concerns, *System Designers* may also require to consult specific SALT references during this stage.

Stage 3: Overall assessment

In order to ensure that the principles of privacy and accountability have been taken into account, the design elaborated in the previous stage has to be evaluated. The SALT Framework provides for this task other questionnaires, allowing to assess the overall system, with respect to its initial aims, and with final checks of legal requirements and ethical and legal proportionality and opportunity. In addition, the SALT Framework allows to verify the system design through the verification of the OCL rules associated to the SALT references for that specific system (if any). To be complete, this third stage should be supplemented by an exhaustive data protection compliance check, which however falls outside the scope of the SALT framework, but that can be performed by legal experts.

In this assessment, not only *System Designers* and *System Proposers* should be involved, but also *System Owners* (stakeholders) to demonstrate their awareness regarding the impacts of the surveillance project on individual's privacy and data protection rights.

Other stages in the system lifecycle

As a result of the three-stage process, a SALT compliant system design is obtained. After this, it is possible to use the SALT Framework during the rest of the system lifecycle for the validation of any modification in the system design or the consultation of changes in the concerns, due for example to the appearance or update of a law.

The following diagram shows a high level description of the whole system lifecycle including the changes mentioned, and grouping together the stages of the system lifecycle that correspond to each of the stages of the 3-stage process mentioned.

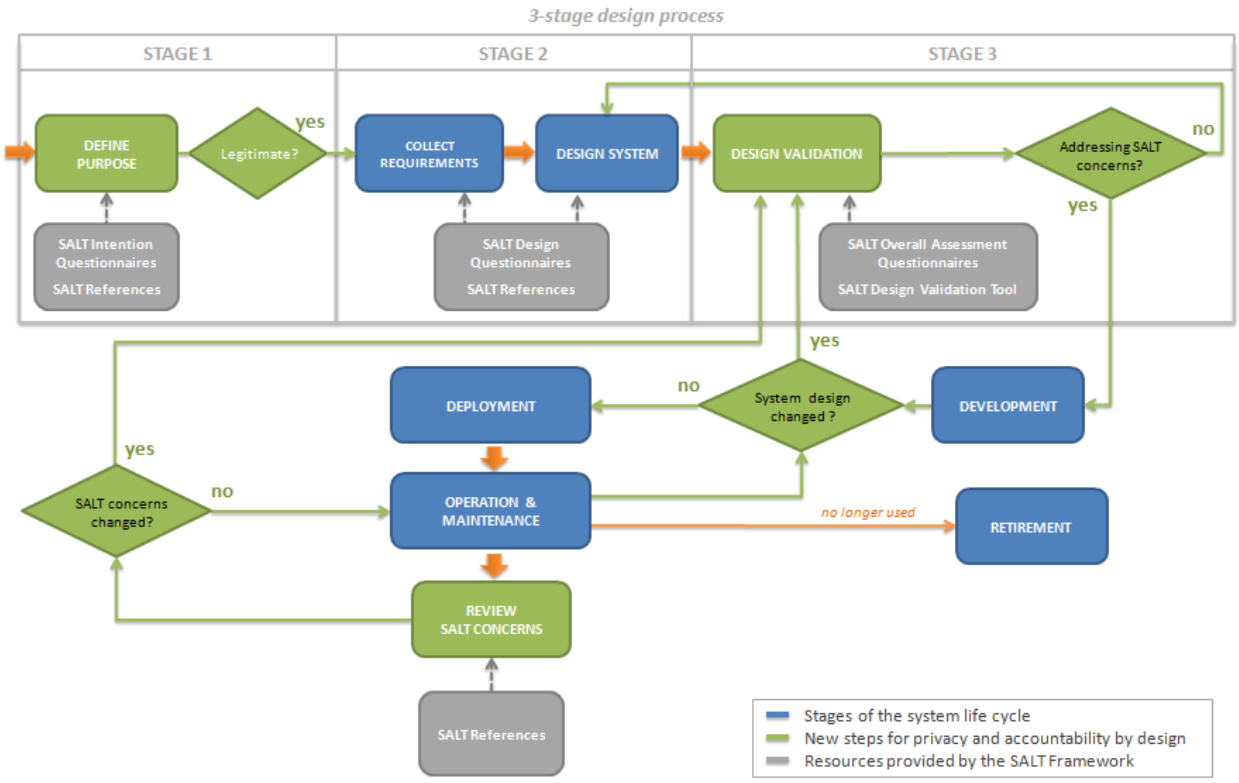

Figure 9: High level description of the lifecycle of a SALT compliant system

This other diagram summarizes the design process including the actors involved at each stage.

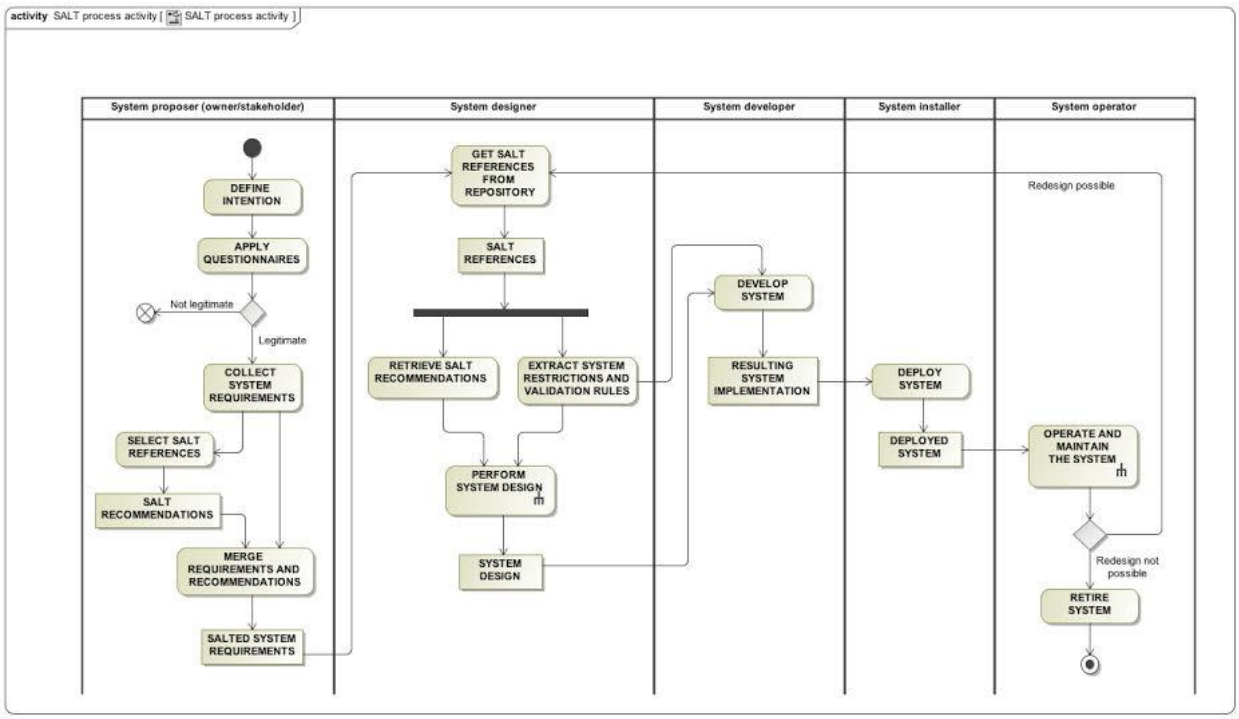

Figure 10: UML activity diagram for the design process of SALT compliant systems

5.2 SALT Framework tools for biometric systems

As illustrated in Figure 9, these are the main resources provided by the SALT Framework:

- **SALT Questionnaires**, allowing to perform different evaluations during the first stages of the system lifecycle.
- **SALT References**, containing concerns and artifacts that can be applied to a specific context, and including in some cases OCL rules that can be used to check the compliance with some concerns.
- **SALT Design Validation Tool**, that allows to model the system in UML format and verify any OCL rule associated.

Below, the different tools are explained.

5.2.1 SALT Questionnaires for biometrics

The questionnaires developed under WP2 will facilitate the identification of the most important concerns on privacy and accountability for the biometric system at an early enough stage to make the right design choices. Although by now all the questions that can be applied to biometric systems are grouped in just one questionnaire (see the example of Appendix A: SALT questionnaire for biometrics), they may be split in the future in smaller questionnaires according to the aim of the questions and the stage of the design process in which they can be applied.

We can find three groups of questions, that may be turned into three different questionnaires, based on the stage of the design process:

- Questionnaires for the evaluation of the system purpose and its proportionality *(Stage 1: Intention)*
- Questionnaires for the guidance of system designers in the elaboration of the design of the biometric system *(Stage 2: Design)*
- Questionnaires for the evaluation of the impact on privacy of the system designed *(Stage 3: Overall assessment)*

In addition, the SALT Framework will store different questionnaires for each type of system. This is mainly because biometric systems are considered more intrusive due to the nature of the data collected, and they are normally regulated by specific legislation or recommendations, therefore, they require a more exhaustive assessment of the procedures and measures implemented for privacy and data protection.

5.2.2 Creation of SALT References

The creation of SALT references is initially delegated to experts in the three different categories considered by the PARIS project, i. e., socio-ethical, legal and technological. Experts are the indicated users because they have the knowledge regarding privacy and accountability concerns for surveillance systems corresponding to each category. This task is achieved via a given functionality of the SFMT (SALT Framework Management Tool), which will show an appropriate interface allowing for non-technological users to interact with the SALT framework (the collection of all SALT references). Thanks to this tool, relevant privacy and accountability information is captured, encapsulated within SALT references and then stored within the SALT repository, the physical media that contains the SALT references.

However, in order to provide a complete SALT reference, i. e. containing all possible information for each concern, not only social, ethical, legal or technological experts are required, but also another type of users is involved: the OCL (Object Constraint Language) expert. Since this type of expert is not mandatory and will not always be available, the SALT repository can store two types of SALT references:

- Complete SALT reference: an OCL expert is available, and hence the SALT reference contains all the information.
- Standard SALT reference: an OCL expert is not available, and hence the SALT reference lacks of the information regarding OCL rules (see section 5.2.4 for an in depth explanation of OCL rules' role).

The SALT reference is the information unit within the SALT repository, and each one contains information regarding one or several privacy and/or accountability concerns. It is important to remark that since SALT references are created by experts, their content fully depends on them. The SFMT ensures that each reference's content is structured and provided to the SALT repository following a predefined format, which makes it appropriate for a digital storage an access. Thanks to this common structure, any social, ethical, legal or technological expert will provide the following information upon the creation of a SALT reference:

- A list (which can be of a single element) of privacy and accountability related concerns for surveillance systems.
- A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc.
- A possible solution (artifact) to address each concern within a given surveillance system design. This information assumes that the system design is provided by means of an UML (Unified Modeling Language) diagram, thus it proposes the what UML artifacts and rationale could be implemented in order to take a given concern into account.

It is noticeable that each concern may be addressed with several solutions, although just a possible one is provided for each concern within a given SALT reference. This means that even though different SALT references may contain the same concern, they may provide different solutions for it, which will fully depend on the expert who creates the reference.

Furthermore, apart from the previous information, if an OCL expert is also available at the time a SALT reference is created, a complete SALT reference will be released also including the following:

- A list of OCL rules (it could be one or several rules). The OCL expert needs to fully understand the meaning of the privacy/accountability concern for which the OCL rules are created. These rules will be of used for the automated (or human assisted) validation of the concern it relates to, once its corresponding solution provided by the SALT reference has been implemented in the system design.

Table 8 shows an example of SALT reference with the information that it can contain.

SALT reference ID	European Community Privacy Principles
Concern ID	Purpose
Description	Clearly define the purpose of processing sensitive data, for which the evaluation of the stakeholder's problem is required
Proposed solution	To describe and justify the purpose of the processing of sensitive data, we extend the UML element representing sensitive data with an attribute called "purpose" as a plain text string to include the evaluation of the stakeholder's problems
OCL rules	**context** Sensitive_data **inv** purpose: not self.legitimacy.oclIsUndefined() Displayed message: Sensitive data must define the purpose of processing sensitive data, for which the evaluation of the stakeholder's problem is required
Concern ID	Legitimacy
Description	Indicate and justify the legal ground on which the implementation of the system relies
Proposed solution	The surveillance system relies in a clear explanation and justification of the legal ground. To express this information we

		expand the UML element that generally represents the surveillance system, which should always exist as an unique element within the system design, with the "legitimacy" attribute
OCL rules		**context** Surveillance_system **inv** legitimacy: not self.legitimacy.oclIsUndefined() Displayed message: Surveillance system must indicate and justify the legal ground on which the implementation of the system relies
		context Surveillance_system **inv** surveillance_system_req: Stereotypes::Surveillance_system::allInstances()->size()=1 Displayed message: The model must contain one and only one Surveillance System

Table 8: Example of content within a SALT reference

Once the process of creation of SALT References and their format is clear, the next step is the translation of the knowledge on privacy and accountability into SALT References that can be used in the design of systems, such as the proposed biometric system of WP6.

Taking into account all the work done so far, what a *System Proposer*, or a *System Designer*, expects to obtain from the SALT Framework is the list of concerns identified in section 3, and at least some of the artifacts described in section 4. This is an example of how the results of sections 3 and 4 can be integrated into SALT References:

- *SALT_Ref_1: Guide on Video Surveillance of the Spanish Data Protection Agency*

Concerns	**Possible solutions**	**Proposed verification / Evidence of compliance** *(to be translated to OCL language if possible)*
REQ_VSS_1	A4	The system could include an attribute to indicate if informative signs are used.
REQ_VSS_2	A2	The main information of a privacy policy could be added as attributes to the biometric system (purpose, responsible person for the processing of personal data, etc.)
REQ_VSS_3	A3	The document informing of the successful resolution of the inscription of the system in the General Register should be kept as evidence.
REQ_VSS_4	A23	An attribute can be required for the cameras, to indicate if the camera covers any public space.
REQ_VSS_5	A2	Any data storage should include an attribute to indicate the retention period.
REQ_VSS_6	A12	Any unit processing personal data should implement data encryption.
REQ_VSS_7	A7	A report of the results of the training sessions must be kept. It could be signed by the attendees.

Table 9: Example of content within a SALT reference based on the requirements of section

5.2.3 Consulting SALT References

SALT references can be consulted by anyone who has access to the SALT repository. However, depending on the type of user, a SALT reference may be accessed and used in a way or another. We can distinguish three main ways of accessing SALT references: merely consulting a SALT

reference, updating its content and using it for a surveillance system design. All these types of access are performed via the SFMT (SALT Framework Management Tool).

To merely consult a SALT reference may be useful to surveillance system proposers (those users interested in the creation of a particular surveillance system). Thanks to this, they can access the SALT repository and check the impact on privacy and accountability of the future system to be, and hence considering its viability (and possible costs overhead).

On the other side, social, ethical, legal and technological experts also need to consult SALT references already stored in the SALT repository. This is not only helpful, but also mandatory in order to keep the SALT references up to date, since privacy and accountability requirements for surveillance systems may change over time. The legal ground could be the first we could think of, since laws are constantly evolving, which leads to a continuous updating process in order to have SALT references that really correspond to real requirements. Nonetheless, it is important to remark that the update process of a SALT reference involves a little more than just consulting the previously stored information. By doing so, the user gets access to the references content, but in case it needs to be updated, the system does not allow for just editing and storing it again. In this case, a new SALT reference has to be created, which can be a copy of the old one with changes in those concerns that need to be modified. After this, a new version of the SALT reference will be saved to the repository, but the old one will also be kept, at least until its final deletion (manually or by an automated process when the expiration date of the reference is reached).

Finally, probably the most concerned user consulting a SALT reference is the designer of the surveillance system. In this way system designers connect to the SALT repository and access those references that are relevant for their particular SUD (System Under Development). Thanks to this, they get information regarding privacy and accountability concerns at design time, achieving a privacy-by-design and an accountability-by-design approach. But not only that, as we have seen in section 5.2.2, they will also have access to possible solutions to handle privacy and accountability within their systems. And on top of that, and automated design validation can also be at their disposal (more about design validation in section 5.2.4). Because of these functionalities, more robust and privacy friendly systems will be finally deployed, since privacy requirements were taken into account from the design phase.

5.2.4 Design validation

Design validation is a tricky task also addressed by the SALT approach, although it is important to make clear that the offered validation support is focused to privacy and accountability concerns, since this is the type of information provided by SALT references. Besides, due to the nature of the handled concerns (laws, policies, social studies, etc.), it is not always possible to provide an automated validation. In these cases where a human action is required to validate the system design, the SALT approach will try to help as much as possible by providing extra documentation to the external auditor in charge of validating the system design. Thanks to this documentation, the auditor will know what parts of the system to look at regarding a concrete

privacy/accountability concern, what methods to check, what attributes should appear, etc. In summary, we try to facilitate the auditor's task.

On the other hand, an automated validation is sometimes available thanks to the OCL rules included within the complete SALT references. These references include a possible solution for a given concern and also an OCL rule that will check whether the proposed solution (that solution and not any other) is accomplished by the system design or not. This validation is performed on-the-fly, meaning that the tool constantly checks the involved OCL rules as the design is being developed. In case an OCL rule is not fulfilled, a message is displayed informing the system designer what concern has not been addressed according to the solution provided by its corresponding SALT reference. At this point, the designer can choose to adopt the proposed solution, preventing from another message appearance, or to ignore it, since he may prefer another known solution. It also exists the possibility of completely ignoring the message by not providing any solution at all. It is important to remember that the SALTed design process has been thought to help developing surveillance system designs, taking into account privacy and accountability concerns. Nevertheless, it is the system designer the person responsible of it, and final design decisions directly lay on him.

The integration of the SALT methodology and design validation within actual industry design processes is achieved via a proposed tool. This tool handles UML diagrams and includes an UML profile that considers the elements that constitute current surveillance systems (video-surveillance and biometric technologies). With this tool, a system designer can drag and drop the proposed elements in order to create a system design, but not only that. The tool integrates an interface that allows for connecting with the SALT repository and access those SALT references containing privacy and accountability concerns that are applicable to the SUD. System designers can keep using the tool in order to apply the solutions proposed by the SALT references while on-the-fly validations are taking place (following a way of operation similar to nowadays software compilers). At the end, SALT compliant system design should be created (in case the system designer decided to take into account the proposed solutions or equivalent ones). Some examples of solutions with their corresponding OCL rules are shown in Table 8.

6 References

[1] Lucas D. Introna and David Wood (2004) “Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems”, In *Surveillance & Society CCTV Special* (eds. Norris, McCahill and Wood) 2(2/3): 177-198

[2] Spanish Parliament, "Organic Law 15/1999 of 13 December on the Protection of Personal Data.", Official State Gazette (1999): 43088.

[3] "Guide on Video Surveillance", © AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (SPANISH DATA PROTECTION AGENCY), Official Publications Identification Number: 052-08-007-8, available online here:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia_en.pdf

[4] Denis Butin and Daniel Le Métayer et al., "End-to-end Privacy Accontability: Systematic Analysis of the General Data Protection Regulation Draft", Inria, Université de Lyon, France, *(document under review).*

[5] ISO/IEC, "Systems and software engineering - Life cycle management - Part 1: Guide for life cycle management", ISO/IEC TR 24748-1:2010(E).

Appendix A: SALT questionnaire for biometrics

I. Opportunity of the system

Purpose

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

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

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

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

Response

The biometric system aims at the detection of unauthorized accesses to the Visual Tools' premises between 9.PM and 7.AM in order to:

(1) Prevent thefts at the office
(2) Facilitate the work of the security guards
(3) Collect evidences for the local authorities in case of incident

Legitimacy

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

Objective of the question:
The European Data Protection Directive 95/46 requires that biometric data (and other kind of personal data) may be collected and processed only under a limited and exhaustive list of circumstances that delineate the legitimate grounds for the processing of personal data.
This means that the biometric system envisaged must necessarily rely on one of the following grounds in order to be valid:

- *Consent of the individuals?*
- *Performance of a task carried out in the public interest?*
- *Legitimate interests pursued by your organization*

You must carefully examine the information provided in relation to each of these situations and assess which one is the most likely to apply in your situation. The sub-questions drafted hereunder will help you to assess whether the envisaged biometric system is likely to be valid or not. If the envisaged biometric system does not find to rely on any of these three situations, it means that it is very likely that the envisaged biometric system will infringe data protection regulation and should therefore be abandoned.

☐ Consent of the individual?
The consent of the individual must be specific, clear and freely given in order to be valid.

The individual's consent cannot constitute a valid ground for the processing of the biometric data envisaged because the persons to be enrolled in the system are employees. As employees, there is a significant unbalance relationship between Visual Tools and its employees: the consent will not be considered as "freely given".

☐ Performance of a task carried out in the public interests or in the exercise of official authority vested in the controller

This is not a valid legitimate ground since Visual Tools is not an official public authority or is not vested with missions of public interests.

☒ Legitimate interests pursued by the organization/person responsible of the biometric system?

The Directive provides that the processing of personal data can be justified where "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject." The controller can rely on such legal ground only when he provides the demonstration that his interests objectively prevail over the rights of the data subjects not to be enrolled in the system.

Biometric access control systems for the security of property or individuals will generally be invoked by controllers as a legitimate interest. However, the Article 29 Working Party considers that such interest only validly justify the use of biometric system under two conditions: (i) In presence of high risks situations and evidence of objective and documented circumstances of the concrete existence of a considerable risk (e.g.:use of fingerprint and iris scan verification to control the access of a laboratory doing research on dangerous viruses.); (ii) after verification of possible alternative measures that could be equally effective but less intrusive).

Response

Visual Tools invoke its "legitimate interests", in particular the protection of its property. Indeed, the biometric system envisaged precisely aims at detecting unauthorized people within Visual Tools' premises at night and by thus aims at controlling who accesses, mainly for the securing of property of Visual Tools.

Two conditions must be met:

☒ There is evidence, on the basis of objective and documented circumstances, of the concrete existence of a risk

Response

In the Visual Tools' headquarters, where the system is going to be deployed, there is a storeroom where equipment of great value is stored (e.g.: manufactured devices, hardware components, software material, etc.). Besides, all the equipment used for the operations of the company is also stored in that location. Therefore, a security system to protect all that material is required.

A video surveillance system has already been deployed there, but it seems insufficient, as some material has disappeared during the night period without anyone noticing, and without being captured by the existing surveillance system.

☒ There is no other less intrusive means available to achieve the security objective (satisfying this condition requires assessing less intrusive means under Q. 6 & 7)

Response

We have considered other solutions but they are not as adequate as the proposed biometric system to detect unauthorized people at the office without interfering with the work of the maintenance employees.

Proportionality

3. Is the biometric system essential to achieve the stated purposes? (Necessity test)

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

Response

It has been proved that the existing system has not been effective enough to protect the goods stored at the office, so an improvement in the security system is required to detect any unauthorized access without interfering with the tasks of the maintenance employees.

After reviewing other existing options, the proposed biometric system seems the most adequate solution considering the good results provided by the bodyprints algorithm in the re-identification of people wearing uniforms in conditions similar to the Visual Tools' premises.

4. Is there evidence that the intended biometric system have produced, in similar other cases or circumstances, the expected effects? (Effectiveness)

The question of effectiveness is closely related to the one of suitability. Efforts to present evidence (when existing), that the intended biometric system has produced the expected effects is important to assess the necessity of the said system.

Response

The technology is quite new, but the evaluations carried out showed a good performance of the bodyprints algorithm for the recognition of people wearing uniforms under conditions similar to the scenario where the system will be deployed.

5. Have other means, in particular non technological means, been considered to achieve the stated purpose(s) ? If yes, which are they? And why have these means been put aside? (Least intrusive means test)

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

Response

These are solutions that were considered to solve the client's problem and discarded:

- *Traditional alarm systems (PIR)*: as there are people working at the office during the defined period, the system would be triggering alarms all time.
- *Control access system based on ID cards*: they can be used to know who has entered in the office through the access control point, but it is not possible to detect or collect information of a person that breaks into the office. Besides, we just want to know if the people inside the office are authorized or not, we don't need to identify or verify them.
- Non-technological solution: *Security guards patrolling the office*. Although a human has the instinct to detect threatening or suspicious situations, it is very difficult for a person to control every corner in a building during a long period, especially if the building is large and has several accesses. Anyway, this solution is too expensive.
- *Video surveillance system & Security guard*: the existing surveillance system is not sufficiently efficient as it does not cover every corner in the offices. Moreover, it is very difficult for just one person to monitor videos from many cameras for a long period of time and also patrolling periodically the premises. This system has been proved to be insufficient, and the cost of having one or two people dedicated to patrol the office all night is too expensive.
- *Video surveillance system & Movement detection:* The movement detection algorithm does not require the collection of biometric data, and it could be used in combination of the videos to extract a list of events where movement is detected and facilitate the task of video search in case of intrusion. But, in this case, as there are people working at the office during the defined period, the system would be triggering alarms all the time.

6. Why do you believe that the biometric system is the less intrusive mean to achieve the stated purpose(s)?

It involves the verification that the intended biometric system does not curtail the right to privacy any more than is necessary to achieve the stated goals. We believe the least restrictive means test should invite the stakeholders to a reflexive approach, where they should argue why other « solutions » have been put aside.

Response

This system collects the same information than other video surveillance systems, the only difference is that it has the capability of extracting biometric features of an individual from the images collected. Those features are stored in the form of bodyprints, which are biometric templates generated from different physical characteristics of the data subject, such as his width or height, and the color of his clothes.

The bodyprints by themselves do not reveal any biometric feature or personal information, being necessary to use the biometric system to identify a person through a bodyprint.

The bodyprints technology has proved to be highly efficient for the re-identification of people wearing uniforms, what makes it suitable for this use case, where only uniformed personnel is authorized to access the office.

To improve the security at the office, we require a tool that facilitates the surveillance tasks of the security guard, helping him to detect any alleged intrusion and to collect evidences for law enforcement. The proposed biometric system will warn the security guard anytime a person is detected and classified as not authorized, being more useful than any motion detection system.

II. Designing the system

General information

7. Which kind(s) of biometrics are used?

Response

The system will rely on bodyprints. A *bodyprint* is a vector of features of a person that uses physical characteristics, such as the height and width of a person and the color of his/her clothes, which are sufficiently distinctive to allow identifying and discriminating people, even with similar clothes.

The bodyprints by themselves do not reveal any personal information. It is necessary to use the bodyprints within the biometric system to recognize a person appearing in the scene.

8. On which one of the following process does the biometric system intends to rely?

☐ Authentication/verification?

The verification of an individual by a biometric system is typically the process of comparing the biometric data of an individual (acquired at the time of the verification) to a single biometric template stored in a device (i.e. a one-to-one matching process).

☐ Identification?

The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one-to-many matching process).

☒ Categorization/Segregation?

The categorization/segregation of an individual by a biometric system is typically the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action. In this case, it is not important to identify or verify the individual but to assign him/her automatically to a certain category. For instance an advertising display may show different adverts depending on the individual that is looking at it based on the age or gender.

Response

Although the system is aimed to find out if a person inside the office is authorized or unauthorized, which is a kind of classification, to achieve that goal the system tries to identify any person detected comparing his template with a database of known people (APDB). Therefore, the system relies on identification.

Interference with privacy rights

9. What types of privacy of the individual does the biometric system potentially impact?

☒ Privacy of the person
☒ Privacy of behavior and action
☐ Privacy of communication
☒ Privacy of data and image
☐ Privacy of thought and feelings
☒ Privacy of location and space
☐ Privacy of association

10. What are the data protection risks generally associated with the use of such biometric system?

Here, it is important to identify the risks that are <u>generally</u> associated with such biometric system. The identification of such risks contributes to the understanding of the technology and its potential impacts on individual's rights. The identification of such risks is also a necessary step of any impact assessment. A correct analysis of the risks could then be used either in view of producing a data protection impact assessment, or as "accountability information".

Response

- *Impact on data protection*
  The impact of the bodyprints technology on data protection is limited, as the bodyprints by themselves do not reveal any biometric feature or personal information, and special capture and processing modules are required to identify a person through a bodyprint. Besides, it is not possible to retrieve the original data (RGB and depth images) from a bodyprint.
- *Identity theft or spoofing*
  In this scenario, someone could try to impersonate the identity of an authorized person. Although the bodyprints technology has provided very good results distinguishing people that wear similar clothes, the possibility of confusing two people with similar aspect and clothes exists.
- *Misuse of the data collected*
  The data collected could be used for other purposes different from the one for which the data was collected (e.g. control the employees working at night, profiling).
- *Accuracy*
  The bodyprints technology provides a low error rate for the re-identification of people wearing uniforms, but errors must be expected. The false positives have more impact on the system performance, as they imply that an unauthorized person has been considered authorized.
- *Revocability / Stability*
  The bodyprints are not very stable in time, as they depend on the appearance of a person at a certain moment or period, therefore they require a periodic review or update to ensure the good performance of the system.
- *Linkabililty*
  The bodyprints by themselves do not reveal any biometric feature or personal data, but in the system designed they are linked to an image (key frame) that can be used to identify a person if it is not properly protected.
- *Consent & Transparency*
  The enrolment of people in the system require the collaboration of data subjects, but the matching process don't, therefore biometric data could be captured without data subjects' knowledge.
- *Unauthorized access to personal data / Disclosure of personal information*
  Someone could try to collect the images or the bodyprints stored with malicious intent (e.g. profiling, identity theft). Only certain users should have access to the information stored in the system for a legitimate purpose.
- *Data tampering / Component manipulation*
  The biometric templates or the different components could be manipulated to modify the results of the categorisation process. Besides, the communications between the different components are susceptible to be interfered, for example to avoid a negative result during the matching phase.
- *Availability*
  Any component is subject to failure, and the system availability can also be reduced through a denial of service attack, which will cause the suspension of the intrusion detection service temporarily or indefinitely.

Suitability and necessity of the type of biometric system

11. Is the choice of the type of biometric system the most appropriate with regard to the purpose(s) aimed at? Why?

Here, it is important to explain the reasons why the choice of a certain type of biometrics appears the most suitable with regard to the stated purpose(s).

Response

Other approaches have been considered, from non-technological solutions to surveillance systems that do not process biometric data, but they have been discarded due to the particular conditions of the scenario proposed, in which there are employees working during the defined period, and the possibility of an intruder breaking into the premises and avoiding an access control point exists.

The bodyprints technology has showed a good performance for the recognition of people wearing

uniforms under conditions similar to the scenario where the system will be deployed. The proposed biometric system based on bodyprints can be used to detect unauthorized accesses without interfering with the work of the maintenance employees, and can also facilitate the collection of evidences in case of intrusion, which makes this option the most appropriate.

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

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

Response

The bodyprints technology allows to classify people without having to identify them. The bodyprints by themselves do not reveal any biometric feature or personal information, and it is not possible to retrieve the data source from a bodyprint (RGB and depth images).

To identify a person through a bodyprint, it is necessary to use the biometric system:

- First, it would be necessary to have a video sequence recorded with a VPU (as a special format is required for the RGB and depth images).
- After that, the video would have to be processed by the same VPU, as the bodyprint algorithm uses the calibration files of the camera used for the capture.
- Finally the results would have to be compared with the bodyprint in the RIS.
- For all this process, local access is required to both devices (VPU & RIS)

Moreover, the bodyprints are different depending on the clothes worn by the data subject, thus a bodyprint can be used with the biometric system to identify a person only if that person is wearing the same clothes.

Taking all this information into account, the bodyprints are clearly less intrusive than other biometric solutions that identify unequivocally a person under any circumstances (e.g. face, DNA, fingerprint), and more respectful with privacy than other non-biometric approaches that require the collection of more personal information.

Enrollment

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

Response

The goal of the enrolment is the extraction and storage of the bodyprints of the authorized people in the Authorized People Database (APDB).

The enrolment is carried out once the system is set up at the Visual Tools premises and properly configured.

This task is managed by the System Administrator (SA), and the process can be summarized as follows:

- The System Administrator captures a video of the person to be enrolled (Authorized Person, AP) with one of the VPUs. As the video should contain enough images to recognize perfectly the AP from different views, this task requires the collaboration of the AP.
- The video created is encrypted and stored in the VPU.
- The extraction and storage of bodyprints can be performed later in the same VPU by the SA, and it does not require the collaboration of the AP (offline enrolment).
- For each video of an AP, several bodyprints will be extracted and a specific user interface will facilitate the selection of the most adequate for the matching phase.
- The bodyprints of the authorized people are stored by the SA in the Authorized People

Database (APDB) located in the RIS.

14. Is the active participation of the individual required?

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

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

☒ **Yes**
☐ **No**

In view of the above comment according to which the active participation of the individual is a preferable option, the enrollment of individuals without their active participation should be explained and duly justified.

If no, why?

Response

-

If no, which safeguards do you put in place to make sure that the persons are aware of their enrollment in the system? How do you organize information of the persons about their rights?

Response

-

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

The amount of data extracted from a biometric source during the enrolment phase has to be adequate to the purpose of the processing and the level of performance of the biometric system. The principle of data minimization means that only the required information and not all available information should be processed.

Response

During the enrolment, the system just collects the data required for the creation of bodyprints: RGB and depth images of the data subject.

16. Are there categories of people that are unable to enroll (young children, elderly people, persons physically disabled)?

Response

No

17. If yes, what are the appropriate safeguards (alternative procedure?) in place for people unable to complete the enrollment process?

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

Response

-

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

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

Response

During the enrolment, the system just collects the data required for the extraction of bodyprints: RGB and depth images of the data subject (video). No other personal information is required.

Matching

19. How is matching carried out?

Response

The goal of the matching phase is the detection of unauthorized people at the defined period (9PM to 7AM).

This task is monitored by the System Operator (SO), and the process can be summarized as follows:

- The VPUs during the defined detection period are continuously analyzing the videos from the depth cameras in order to detect the people appearing in the scene and to extract their bodyprints.
- The RIS in this phase collects periodically the new bodyprints from the VPUs, and compares them with the APDB. Any result, positive or negative is temporary stored in the Results Database (RDB) until it is verified by the system operator.
- The System Operator can monitor and validate the results of the recognition process using a specific user interface, and in case of intrusion, the SO is responsible for reporting the incident to the local authorities.

20. Is the active participation of the individual required?

As it is the case during the enrollment phase, the active participation of the individual during the matching phase, whenever possible, constitutes a preferable option since it is a good opportunity for him/her to be aware of the processing of his/her biometric data.

☐ **Yes**
☒ **No**

If no, why?

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

Response

The system uses the images captured by the video cameras to automatically extract the bodyprints of the people appearing in the scene, that are compared with the database of authorized people (APDB) without any user interaction. Thus, the matching can be performed without the collaboration of the data subjects.

The people that is allowed to be at the office at the defined matching period, has already been enrolled in the system, and therefore they should be already aware of the biometric system.

Besides, we have placed several informative signs at the entrance of the areas under surveillance informing about the existence of a surveillance system. And the employees of the company will be informed about the new capabilities of the surveillance system.

Finally, we cannot expect the collaboration of intruders during the matching phase.

Accuracy

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

The False Accept Rate (FAR): It is the probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. It measures the percentage of invalid inputs which are incorrectly accepted. It is also known as the false positive rate.

The False Reject Rate (FRR): It is the probability that the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. It is also known as the false negative rate

Response

As this technology is quite new, and it has not been used yet for this purpose, we don't have enough information to define the performance evaluation metrics for the system.

Anyway, we have performed different tests to determine if the approach based on bodyprints is effective enough for the goal pursued:

Technology testing in a laboratory environment, that served to evaluate the bodyprints algorithm for re-identification, with these results:

- The average correct re-identification performance obtained was 93% (IR) with bodyprints obtained always from the same view (frontal or rear).
- The average correct re-identification performance obtained was 55% (IR) with bodyprints obtained from any view (frontal or rear). The main problem here was the existence of logos in the clothes that appear in one view but not in others, which increased the number of false negatives.

Scenario testing: we have carried out several tests in a controlled scenario with conditions that are similar to the environment where the system will be installed, in which the test system tries to recognize people wearing uniforms:

- The average correct re-identification performance obtained was 98.5%, with bodyprints from different views. We could also observe that the system distinguished perfectly different people wearing the same uniform.

22. Is this FAR and FRR acceptable? Why?

Response

The evaluations showed a good performance of the bodyprints algorithm for the recognition of people wearing uniforms under conditions similar to the scenario where the system will be deployed.

Besides, the biometric system is aimed to be an aid in the surveillance tasks of security guards, which means that whatever the results of the recognition process, there will be a human verifying the alarms, so the impact of a failure in the matching process can be reduced or mitigated.

In the different tests carried out, most of the errors during the matching were false negatives, that means that the system didn't recognize a person whose bodyprint was stored in the template database. This type of errors will make the defined biometric system to generate an incorrect alarm, that will be discarded by the system operator in charge of monitoring the office, so this type of errors are acceptable.

In the proposed scenario, the main risk in the recognition process is obtaining a false positive, meaning that an unauthorized person has been classified by the system as authorized. In light of the results of the tests performed, this type of errors are least likely to occur. Moreover, the matching is performed several times for each person appearing in the scene, increasing the probabilities of detecting correctly an unauthorized person.

Finally, in order to detect inaccurate bodyprints stored in the template database (APDB), the number of false negatives for each bodyprint stored in the APDB will be monitored.

Access/disclosure conditions

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

Response

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

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

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

Response

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

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

Technical measures mitigating data protection risks

The Working Party has identified technical and organizational measures aiming at mitigating data protection and privacy risks, that can help to prevent negative impacts. These technical measures aim in particular at mitigating the risks of identity fraud, the risk of purpose diversion (or function creep) and the risk of data breach. Following the identification of the level of data protection risks raised by a type of biometric, the organization should assess carefully the opportunity to recourse to some of the technical measures discussed in the questions below.

STORAGE

25. 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.

☒ **Yes**
☐ **No**

Response

The system stores the biometric data in the form of bodyprints, that are biometric templates.

To facilitate the verification of alarms, a key frame (image) will also be stored in the RMS. This frame will be protected by encryption.

26. 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.

Response

To obtain the bodyprints, images of the full body are used, being possible to extract bodyprints of a person from a video sequence showing only one view (e.g. frontal view).

Anyway, it is not possible to recover the original RGB and depth images from a bodyprint. The process of extraction of bodyprints is not reversible, as it uses several images of a person in different moments, and it depends on how a person moves.

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

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

☐ **Yes**
☒ **No**

Response

No, it is not possible to recover the RGB and depth images from a bodyprint, the process is not reversible.

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

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 centralized 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 unauthorized 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 unauthorized access. Furthermore such decentralized 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 centralized database covers a wide range of technical implementations from the storage within the reader to a network hosted database.

☐ **The data are stored on a device carried by the individual**
☒ **The data is stored in a centralized database**

Response

The bodyprints and key frames of the authorized people are stored in a centralized database located in the RIS (APDB). The group of authorized people is composed of a maximum of 10 people, so the template database is not large. The access to the APDB is controlled and traced, being required administrator privileges to add, update or delete the templates, or to see the key frames of the authorized people.

On the other hand, the bodyprints extracted during the matching phase are temporary stored in the VPUs, until they are collected by the RIS for the comparison of templates. Once in the RIS, the new bodyprints are deleted after the comparison with the template database. The results of the comparison and the key frames are kept in a temporary storage (RDB) until they are verified by the system operator. The access to this temporary storage is controlled and traced, being required operator or administrator privileges to access the data.

With the system designed, the only way to check at any time if a person detected is authorized is comparing the new bodyprint with a set of bodyprints of authorized people, which cannot be performed with a portable data storage (ex: ID cards including the bodyprints), especially if the data subject is an intruder that has broken into the office.

RETENTION PERIOD AND DELETION/ERASURE

29. Are the raw data deleted after the template is generated?

☒ **Yes**
☐ **No**

Response

During the enrolment, the raw data (RGB and depth images) are stored in a VPU until an adequate bodyprint has been extracted for the data subject to be enrolled in the system. After that, all the images are deleted except one that is used as a key frame that facilitate the verification of alarms. This key frame is encrypted, being required administrator or operator privileges to see the images in the clear. This process is managed by the System Administrator.

During the matching phase, the RGB and depth images are analysed “on the fly”, meaning that the images are immediately deleted after they have been analysed, except the image used as key frame of a bodyprint, that is adequately encrypted. This process is automatic.

30. How long is stored the biometric data? Why is such retention period considered as necessary?

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

Response

The RGB and depth images (videos) from which the bodyprints are extracted is stored for different periods depending on their purpose:

- For enrolment, the videos are stored in a VPU until an adequate bodyprint has been extracted for the data subject to be enrolled in the system.
- For matching, the video frames are deleted right after processed. This task takes only a few seconds after a frame has been loaded for analysis, and the deletion is automatic.

With each bodyprint, a key frame is saved to facilitate the verification of alarms. These key frames are encrypted, being required administrator or operator privileges to see the images in the clear.

Both the key frames of the authorized people database and the bodyprints are kept in the system until the corresponding data subject is unenrolled, or until the system is retired, as they are required during the operation phase of the system lifecycle for the detection of unauthorized people.

The bodyprints of the data subjects appearing in the office during the matching phase are deleted once the comparison is performed, and the key frames are kept a little longer, until the results of the recognition are verified by the system operator, with a maximum limit of one month.

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

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

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

☒ Yes
☐ No

Response

DELETION PROCEDURES

RGB and depth images (videos):

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

Bodyprints extracted for enrolment:

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

New Bodyprints extracted during the matching phase:

- In the VPUs, the bodyprints have to be first marked by the RIS as "collected". A scheduled process in each VPU will periodically review the bodyprints and will delete those marked as "collected". Besides, each time a VPU is switched on for matching, all the temporary storages containing images and bodyprints are automatically cleared.
- In the RIS, the new bodyprints collected for matching are deleted automatically right after the comparison has been performed.

Key frames:

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

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

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

SECURITY

32. Are the biometric data stored in encrypted form?

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

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

☒ **Yes**
☐ **No**

Response

Although it is not possible to recover the RGB and depth images, or to retrieve any biometric feature from the bodyprints, they will be encrypted to prevent their misuse (e.g. to manipulate the comparison performed in the RIS and get always a positive match).

The key frames, will also be encrypted.

33. Have you implemented anti spoofing measures?

To maintain the reliability of a biometric system and prevent identity fraud the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person. In respect of facial recognition, it may be critical to ensure that the face is a real one and not for example, a picture tied on an impostor's head.

☒ **Yes**
☐ **No**

Response

There are a few ways to perform identity fraud in this scenario:

- *Copying the biometric features of an authorized person*: the system based on bodyprints is able to distinguish two people wearing the same uniform with a high probability. To impersonate the identity of an enrolled person it would be necessary to copy his clothes, his proportions and his gait, that is almost impossible. Anyway, the results of the matching process have to be reviewed by a human operator, therefore this risk can be avoided or mitigated.
- *Introduce in the APDB the bodyprint of a non authorized person*: for this it is necessary to generate a bodyprint of the person, and then store it in the RIS. This requires local access to the RIS, and to one of the VPUs, with administrator privileges. To control this, the collection of data and any access to the APDB is traced.
- *Manipulation of the matcher (RIS)*: another way to be accepted as authorized is to modify the configuration of the matcher and reduce the threshold to consider any result as positive match. As all the results have to be reviewed by a human operator, this risk can be avoided or mitigated. Besides, any change in the RIS configuration will be traced.

On the other hand, in order to detect inaccurate bodyprints stored in the template database (APDB) and maintain the reliability of the system, the number of false negatives for each bodyprint stored in the APDB will be monitored. A high rate of false negatives for a bodyprint is an indication of low accuracy.

34. Do you use biometric encryption?

Biometric encryption is a technique using biometric characteristics as part of the encryption and decryption algorithm. In this case, an extract from biometric data is generally used as a key to encrypt an identifier needed for the service.

This system has many advantages. With this system, there is no storage of the identifier or of the biometric data: only the result of the identifier encrypted with the biometrics is stored. Moreover, the personal data is revocable as it is possible to create another identifier that can be protected with biometric encryption as well. Finally, this system is more secure and easier to use to the person: it solves the problem to remember long and complex passwords.

However, the cryptographic problem to overcome is not easy because encryption and decryption are intolerant to any changes in the key, whereas biometric provides different pattern which may give rise to changes in the extracted key. The system must therefore be able to compute the same key from slightly different biometric data, without increasing the False Acceptance Rate. The Working Party agrees that Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

☐ **Yes**
☒ **No**

Response

The access to the template database (APDB) is traced and controlled by authentication and authorization mechanisms, and the bodyprints will be encrypted, but we will not use this technique.