



PrivAcy pReserving Infrastructure for Surveillance

Deliverable D5.2

Video Surveillance Lifecycle Management Use Case SALT compliant Framework

Project: PARIS
Project Number: SEC-312504
Deliverable: D5.2
Version: v0.1.
Date: 30/12/2014
Confidentiality: restricted to PARIS consortium
Authors: Mathias BOSSUET,
Michel PROMONET (THALES)
Zhendong MA, Daniel HOVIE,
Christian WAGNER, Stephan VEIGL (AIT)
Claire GAYREL (UNamur)
Fanny COUDERT (KUL)
Daniel Le-METAYER & Vinh-Thong TA (INRIA)



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

Table of Contents

DOCUMENT HISTORY	4
EXECUTIVE SUMMARY	4
LIST OF TABLES.....	6
ABBREVIATIONS AND DEFINITIONS.....	7
1 INTRODUCTION	8
1.1 DELIVERABLE OBJECTIVES AND SCOPE	8
2 OVERVIEW OF THE WP5 VAS USE CASES	9
2.1 HIGH LEVEL DESCRIPTION OF SCENARIO AND ACTORS	9
2.2 SYSTEM ARCHITECTURE FOR THE USE CASES	10
2.3 OVERVIEW OF THE 2 WP5 USE CASES	13
2.4 VIDEO ARCHIVE SEARCH PROJECT -- ADVISE	14
3 SPECIFICATION OF SALT FRAMEWORK FOR VAS USE CASE.....	15
3.1 METHOD FOR THE SPECIFICATION OF SALT FRAMEWORK	15
3.1.1 General picture	15
3.1.2 Correspondence with the 3 stage design process.....	20
3.1.3 Specification of SALT references in this document	21
3.2 LEGAL ARTIFACTS.....	22
3.2.1 Introduction to legal requirements about video-surveillance	22
3.2.2 Structure of legal references in this document.....	24
3.2.3 Table of proposed legal references in this document.....	25
3.2.4 Access to images by law enforcement authorities in Belgium.....	28
3.2.5 Access to image by public forces for investigation purposes in United Kingdom.....	29
3.2.6 Video surveillance in France.....	30
3.2.7 Law Enforcement Data Protection Directive.....	37
3.2.8 General Data Protection Regulation	49
3.3 SOCIO-ETHICAL ARTIFACTS.....	52
3.3.1 Introduction to Socio-Ethical artifacts.....	52
3.3.2 Table of proposed Socio-Ethical artifacts in this document.....	53
3.3.3 2008 CNIL study: “French people and videosurveillance”	55
3.3.4 “surveillance ethics” from Internet Encyclopedia of Philosophy (IEP)	58
3.3.5 “video surveillance research in retailing: ethical issues”	60

3.4	TECHNICAL ARTIFACTS.....	61
3.4.1	Introduction to technical artifacts.....	61
3.4.2	Table of proposed technical artifacts in this document.....	62
3.4.3	France - Security Guide (CNIL).....	63
3.4.4	Denial of Service risk and possible remediation	65
3.4.5	Encryption of video data	66
3.4.6	Access-control to video-surveillance systems.....	67
3.4.7	Capabilities of Google Glass cameras.....	69
3.4.8	Operators actions logging.....	70
3.4.9	Resolution of video images and recognition performances	71
4	SPECIFICATION OF VAS USE-CASE 1 AND RISKS RELATED TO PRIVACY AND ACCOUNTABILITY	73
4.1	SPECIFICATION OF VAS USE CASE 1: PRIVACY-PRESERVING LAW ENFORCEMENT ACCESS TO VIDEO ARCHIVE SEARCH	73
4.2	RISKS LINKED TO USE-CASE 1	79
5	SPECIFICATION OF VAS USE-CASE 2 AND ASSOCIATED RISKS TO PRIVACY AND ACCOUNTABILITY	86
5.1	SPECIFICATION OF VAS USE CASE 2: ACCOUNTABILITY OF OPERATORS.....	86
5.2	PRIVACY AND ACCOUNTABILITY RISKS LINKED TO USE-CASE 2.....	92
6	CONCLUSION	95
7	REFERENCES	96

Document History

Version	Status	Date
V0.1	First version, with table of contents and preliminary contents from Thales and AIT	19/11/2014
V0.4	Augmented draft version with Thales, AIT, NAMUR, KUL contributions ready for internal review	17/12/2014
V0.5	Augmented version with Namur and KUL contributions ready for review	18/12/2014
V1.0	Version slightly augmented (KUL) and finalized following reviews from Namur, KUL, AIT and UMA	26/12/2014

Approval		
	Name	Date
Prepared		
Prepared		
Prepared		
Authorised		
Circulation		
Recipient	Date of submission	
Project partners	day/month/year	
European Commission	day/month/year	

Executive Summary

This deliverable D5.2 “video surveillance lifecycle management use case SALT compliant framework” is at the cornerstone of the works performed in most of the work-packages of the project; this is equally true for the D6.2, dedicated to the application of the SALT methodology and processes to a biometrics use case.

Both deliverables rely on WP2 “concepts of SALT frameworks”, WP3 “SALT frameworks management tools”, and WP4 “SALT compliant processes”, work-packages which are themselves under progress.

In this deliverable, SALT example contents are proposed about video-surveillance following 2 main goals:

- To provide exemplification of contents for the sake of awareness, but also to enable to refine the SALT tools and processes by raising discussion and convergence on concrete matters within (and outside of) the multi-disciplinary PARIS consortium,

- To provide usable concerns for the balance of the 2 use cases proposed in the scope of the WP5 (both related to video surveillance systems).

The 2 cases are themselves refined in this deliverable (the first one aims at emphasising privacy concerns whereas the second is more dedicated to accountability), especially about the risks they carry upon privacy.

These contents will be, during the last 12 months of the project evolved if necessary, and secondly integrated in the concrete SALT tools developed. Then, the concrete use in the field of the use cases will enable to raise feedbacks and potential improvement options over PARIS methodology and tools.

List of Figures

Figure 1: Approach to SALT development for the use case	8
Figure 2. Hierarchical structure of the actors for the use cases	10
Figure 3: high-level architecture of the system	11
Figure 4: system architecture for the use cases	13
Figure 5: SALT framework use guidelines [from WP4]	15
Figure 6: Internal contents of the SALT framework per system type	16
Figure 7: SALT reference example presentation for editing using the SFMT	18
Figure 8: Integration of SALT framework to system development life cycle	19
Figure 9: 3 stage process [from WP2]	21
Figure 10: 3 stage process application using the SFMT	21
Figure 12: perception of video-surveillance cameras by the French population (from [2])	55
Figure 13: perception of the importance of the surveillance in public space by French population (from [2])	56
Figure 14: general agreement about the installation of video-surveillance cameras in the French population (from [2])	57
Figure 15: photography of Google glasses (from en.wikipedia.org)	69
Figure 16: impact of image resolution upon the potential performance of a video-surveillance system	71
Figure 17: authentication panel to PEAC, Privacy Enhanced Access Control	75
Figure 18: access to video-surveillance cases panel	76
Figure 19: automatic persons detection and extraction principle	76
Figure 20: Police Officer activity diagram for VAS use case 1	77
Figure 21: data flows at stake within use case 1	78
Figure 22: graphical summary of VAS use case 1 misuse cases	85
Figure 23: illustration about the auditing process about the operators' actions	89
Figure 24: illustration about live and recorded video management system	90
Figure 25: illustration about the auditing tools for the operators' actions	92

List of Tables

Table 1: applicability of Legal SALT references to the WP5 Use-Cases	28
Table 2: list and applicability of SALT Socio-Ethical references to the WP5 Use-Cases	54
Table 3: contents of technical references and their applicability to WP5 use cases	63

Abbreviations and Definitions

Abbreviation	Definition
CAGR	Constant Annual Growth Rate
CCTV	Closed Circuit Television
CONOPS	Concept of Operations
CNIL	Commission Nationale Informatique et Libertés
FPS	Frames Per Second
ECHR	European Convention on Human Rights
HMI	Human-Machine Interface
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technologies
IP	Internet Protocol
LAN	Local Area Network
NAF	NATO Architecture Framework
NVR	Network Video Recorder
OS	Operating System
OSI	Open Systems Interconnexion
PARIS	PrivAcY pReserving Infrastructure for Surveillance
PET	Privacy Enhancement Technology
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PII	Privacy Identifiable Information
PPOF	Privacy Point Of Failure
PTZ	Pan Tilt Zoom
SALT	Socio-ethicAl, Legal, Technical
SGDSN	Secrétariat General de la Défense et Sécurité Nationale
SPOF	Single Point Of Failure
VCA	Video Content Analysis
VLAN	Virtual LAN
VMS	Video-Management System
WAN	Wide Area Network
WP29	Article 29 data Protection Working Party

*[The content is indicative and subject to change through the writing process of this deliverable.]

1 Introduction

1.1 Deliverable Objectives and Scope

The aim of the WP5 use cases is to demonstrate how to use the SALT framework while designing and operating a privacy-preserving video archive search system and the gains of this framework on the positive privacy protection/surveillance performance global sum.

This deliverable provides SALT information (SALT references) especially suited to the VAS and the video data surveillance lifecycle management contexts.

This deliverable also provides a refined description of the 2 use cases proposed to illustrate this thematic of VAS (Video Archive Search) and video surveillance data management. For each of them, it provides a set of possibly problematic scenarios that would lead to abnormal consequences of the use of the system among the following possible issues:

- Potential privacy impacts,
- Limitation of the expected accountability of the stakeholders,
- Downgrade of the surveillance performance of the system.

The concrete development of the use case is the main topic addressed within the task 4 of the WP5 “SALT compliant Use Case development”, which will be documented in the D5.3 “Video Surveillance Lifecycle management use case”. The evaluation through the use cases, of the SALT approach (methodology and tools) is covered within the task 6 (Evaluation of Framework and Framework Management Tool) and within the task 7 (Evaluation of design process).

The whole approach is iterative, each step giving rise to feedbacks on the SALT tools and contents, as shown below.

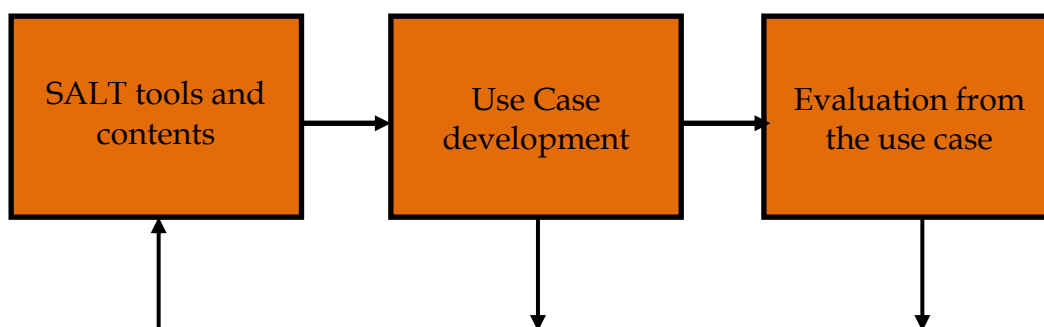


Figure 1: Approach to SALT development for the use case

2 Overview of the WP5 VAS Use Cases

2.1 High level description of scenario and actors

High level scenario

Video archive search (VAS) searches large amount of video data for incident investigation, which usually involves search, analysis, and collection of video surveillance data from the crime scene.

The video data are captured and stored in surveillance systems deployed at various geographic locations and operated by different organizations. Network Video Recorders (NVR) are used in these systems to store video input from cameras over networks. In the same way, the video data in the NVRs can be remotely accessed over the IP network. Video Management Systems (VMS) are used to manage the access of operator stations to the video data in NVR.

To be more efficient in protecting public security and combating crime, the law enforcement agency considers using video search technologies to facilitate crime investigation. The law enforcement agency works together with technology providers and surveillance system operators to design and develop an advanced video archive search system that can access and search video data in various NVRs, while ensuring privacy and accountability by design to eliminate privacy risks at all levels.

The project will use the SALT framework to address all concerns related to socio-ethical, legal, and technical aspects in the design and development lifecycle.

Actors

Actor specifies a role played by a human user or any other system that interacts with the technical system under consideration.

A list of the actors possibly implied in the use cases is given below.

- Law Enforcement Agency (**LEA**) refers to police agency responsible for social order and public safety.
- Police Officer (**PO**) is a member of the LEA, who investigates crime.
- Infrastructure Provider (**IP**) is an organization providing infrastructure to the public and employing video surveillance for physical security of its perimeter. From a legal point of view, he is also considered as the Controller, the one responsible for video surveillance operation and the one who determines the purpose and means of processing video data. We treat IP and Controller equally, as the latter term is referred to in EU data protection law.
- **Operator** is a staff member of the IP, who operates the video surveillance system.

- Data Protection Officer (**DPO**) is a person appointed by the IP to ensure privacy and data protection compliance with regulation.
- Data Protection Authority (**DPA**) is an independent governmental authority charged with ensuring compliance with data protection law, assuming the role of the supervisory authority for a country.
- Technology Provider (**TP**) is a company providing technical solutions related to video surveillance and video archive search.
- **Engineer** is a person employed by the TP. The term is used collectively to refer to any technical staff including designers, developers, and technicians.
- **Citizen** is an individual of the general public, who might be captured by the surveillance systems. Following data protection law, Citizens are data subjects with respect to their personal data processed by video surveillance systems.
- **Victim** is a person, who is a target of a crime.
- **Suspect** is a person suspected of committing a crime.
- **Judge** is a person or a panel, after presented with request and evidence of a case, issues a ruling on the matter.
- SALT Experts (**SE**) is a group of experts maintaining the SALT framework.

The hierarchical structure of the actors is shown below.

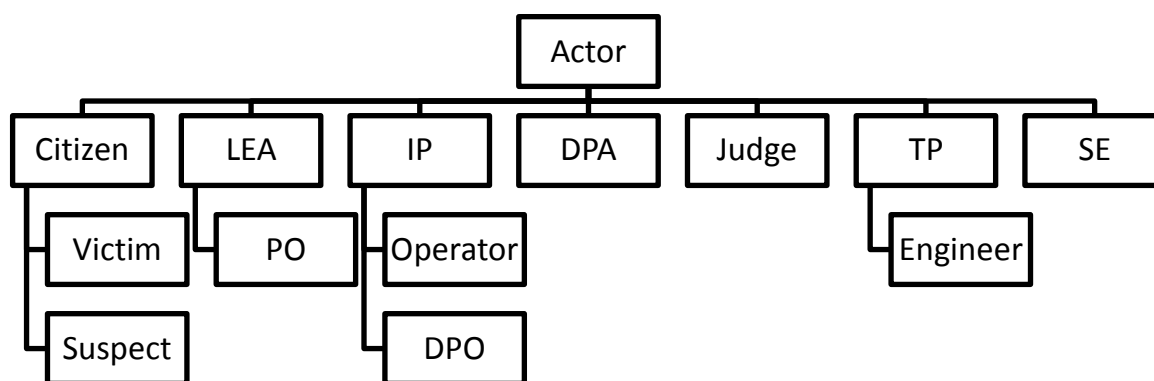


Figure 2. Hierarchical structure of the actors for the use cases

2.2 System architecture for the use cases

System design overview

A technical view of the system is given below. From left to right, there are the NVR at the infrastructure provider storing all video data captured by cameras deployed at its premises, the VAS server developed and hosted by a contracted technology provider, and the video archive

search front-end at the law enforcement agency. Data are exchanged in secured channels, possibly over the Internet.

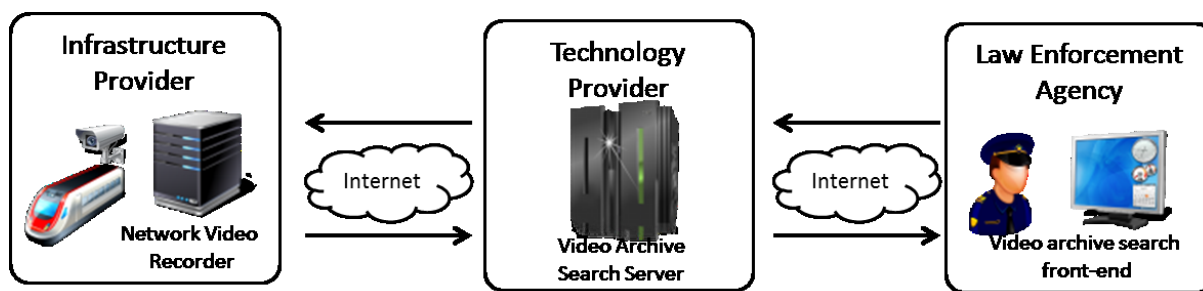


Figure 3: high-level architecture of the system

To provide the desired functions, the team project (including members of the IP, TP, and LEA) proposes a system architecture design that fulfils the functional requirements for video archive search, as well as non-functional requirements on privacy and security.

The Figure 4 below shows the conceptual view of the system, which includes system components, actors, and their interaction with the system. The system is distributed within different organizational boundaries, including the Infrastructure Provider (IP), Technology Provider (TP), Law Enforcement Agency (LEA), and competent Jurisdiction.

- The IP hosts the NVR, announces the information on the available cameras and provides means to operators (including police) to access raw video files, real-time or recorded video data. These means are typically referred to as VMS (Video-Management System). The NVR also hosts some capabilities to synchronously record other types of data, such as audio streams, or metadata's streams (internal or external to the system). It also hosts authorization and access control to the cameras and streams. Within the field of the PARIS project, this access control capability is enhanced, a recording mechanism and a graphical tool for the audit of the operators actions is developed. Also, a tool for assessing the age of the videos present in the system is developed.
- The TP, which has the main responsibility for the design and development of the VAS system, has proposed a solution that includes the video archive search, the component PEAC (Privacy prEserving Access Control), and a database that stores digitalized search requests (including simple PO search requests or judiciary search warrant if applicable) and the information on available video sources. The PEAC is based on the XACML data flow model defined by OASIS¹.
- The LEA implements the "four eyes" mechanism: a DPO interprets video search request (paper written), configures the access control policy for a PO for the specific related case. The PO can only configure and perform video archive search according to the pre-defined access control policy.

¹ <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html>

- If required under national law, the Judge, upon a request for video archive search from a PO, may decide its legitimacy and issue a “video search warrant” accordingly, on a case-by-case basis.

Note that there are several databases in the proposed system design, including:

- Requests database stores digitalized video search requests. This database is used as a basis for access control policy. It also keeps a copy of the available video data source denoted as available cameras from the IP.
- User database. This is the local identity management (IdM) information at the LEA. The PEAC can leverage the IdM for authenticating the users at LEA (i.e. a PO or a DPO).

There are also several users interface at the LEA that interact with the components for VAS system, including:

- A Video-Management System client for the PO. It enables to control the video system, and to watch live and recorded streams, without advanced intelligent processing,
- A VAS Client for PO. It's a user interface for a police officer to compose a video archive search workflow and perform the search (see “Video archive search user story” for more details).
- A browser for DPO. This user interface is the primary place for a DPO to specify the privacy-preserving video archive search policy based on the paper search request. It actually functions like a policy authoring point.

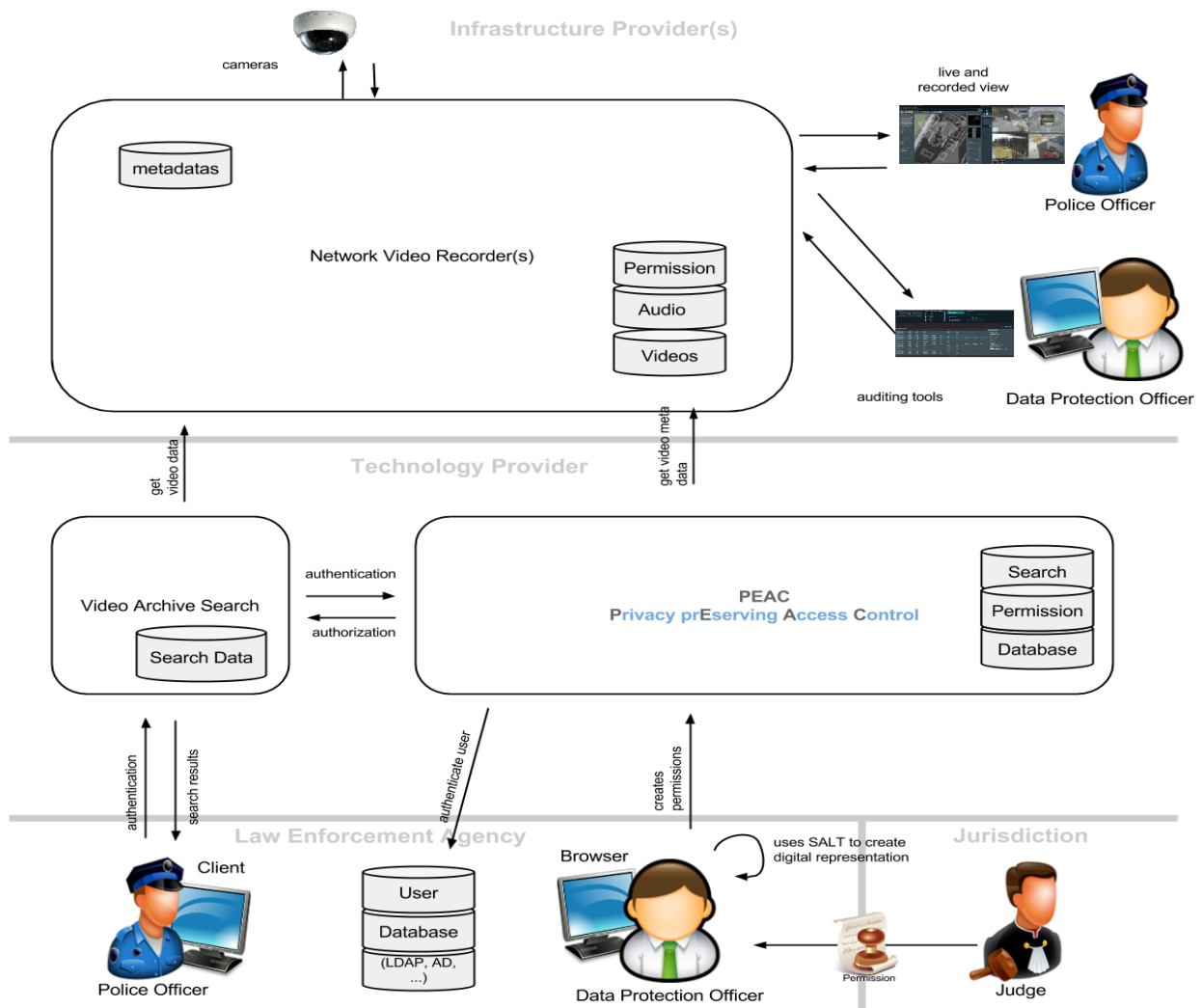


Figure 4: system architecture for the use cases

2.3 Overview of the 2 WP5 use cases

2 use cases are proposed in the scope of the WP5 of the PARIS project: a first use case is mainly dedicated to the demonstration about privacy protection mechanisms. The second use-case focuses on accountability-enforcing mechanisms and benefits.

An imaginary scenario illustrates each of the use-cases:

- Use case 1 scenario is based on a workflow related to the request by a PO or a judge of a video footage related to a specific crime scene in the frame of a criminal investigation (following a complaint from an individual). The risks identified are mainly related to the privacy possible impacts raised by possible non-authorized disclosure of video footages,
- Use case 2 scenario is based on a crime that is committed within the field of a surveillance camera, likely to be detected in real-time by operators, but that has not caused any alarm.

The use case enables considering possible accountability mechanisms that may help tracing how the system was used while the crime was happening.

Privacy- and accountability- enhancing technologies are proposed within these use cases.

2.4 Video Archive Search project -- ADVISE

During the PARIS project, the consortium has identified an EU FP7 project: Advanced Video Surveillance archives search Engine for security applications (ADVISE), which share some commonalities with our WP5 use case.

The ADVISE project aims to design and develop an open and extensible framework to help law enforcement authorities for efficient evidence search in multiple and heterogeneous video archives. According to ADVISE D3.1 Use case analysis and user scenarios, the use cases defined in the ADVISE project covers law enforcement investigation of the cases related to:

- Beat and run away
- Threat or pick pocketing
- Vandalism against parked vehicle
- Stealing of fuel.

The ADVISE solutions achieve these goals by using geo-tag for video archive retrieval and advanced video analytics algorithms for event detection. For legal, ethical, and privacy considerations, the ADVISE project conducted a Privacy Impact Assessment and developed privacy-preserving video analytics.

Although there are some similarities between the ADVISE project and the WP5 use case on video archive search and chosen use case (i.e. law enforcement crime investigation), the two approaches differ in the following ways:

1. The ADVISE project is dedicated to technologies for video archive search, while the WP5 use case is only one part of the PARIS project, focusing on demonstrating the application and value of the SALT framework.
2. The ADVISE project focuses on achieving privacy by developing advanced video analytics algorithms, while the WP5 use case focuses on achieving privacy by system design.
3. The ADVISE project looks at a solution specific the video archive search system developed in the project, while our objective is to have a generic solution.

Nevertheless, the ADVISE use cases provide us with valuable input and inspiration to fine-tune our use case and scenarios. It should be noted that a link has been established between PARIS and ADVISE. The partners from PARIS were invited to attend the ADVISE Liaison Workshop, held in Pont-Saint-Martin, Aosta, Italy on 24-26 November 2014. It is foreseen that the PARIS project will keep liaison activities with ADVISE during its project time.

Details of the ADVISE project can be found on its web site <http://www.advise-project.eu/>.

3 Specification of SALT framework for VAS Use case

3.1 Method for the specification of SALT framework

3.1.1 General picture

The SALT framework enables to store information about surveillance systems and to retrieve the relevant information for a specific surveillance use case. Some of the information pieces embedded within the SALT framework contain specifications and restrictions about the surveillance system itself or about one or several of its components. Under some conditions, these specifications and restrictions can be verified automatically. The main conditions for this are:

- The surveillance system design shall meet the design guides embedded within the SALT framework.
- The constraints shall be expressed towards the system design using OCL rules.

The dynamics and process for the usage of the SALT framework is depicted below, using a diagram coming from the Work-Package 4 of the project (SALT compliant process).

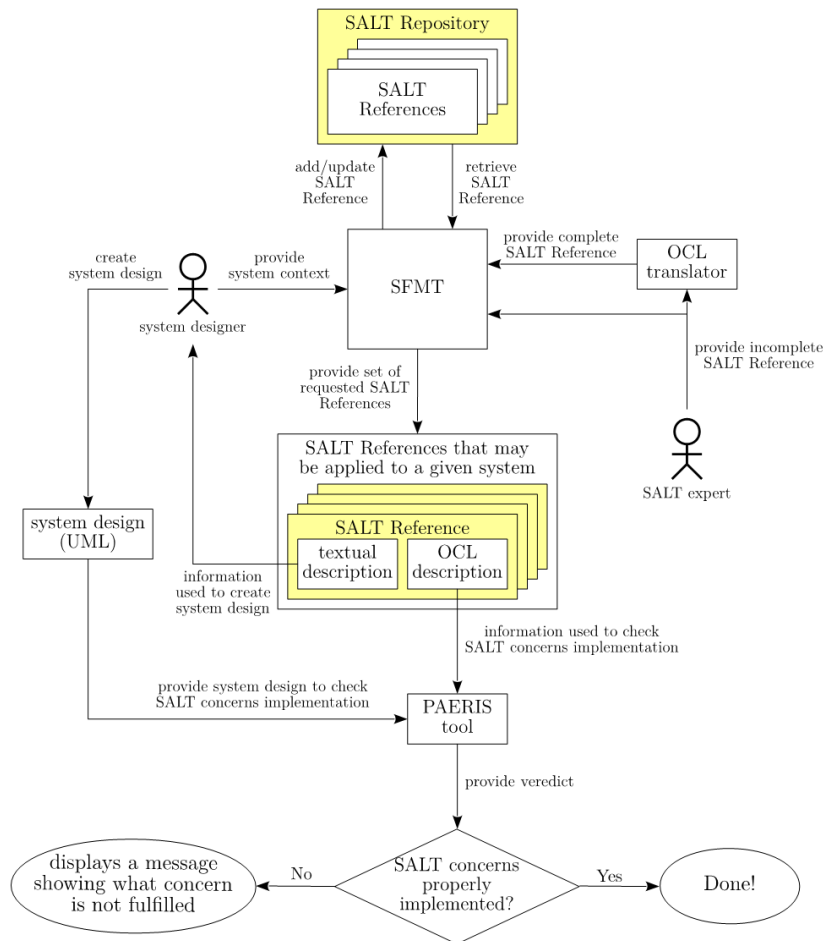


Figure 5: SALT framework use guidelines [from WP4]

The atomic content of the SALT framework (dedicated to the storage of the information pieces) is the SALT reference. The SALT framework also contains 2 other types of entities:

- Systems profiles (UML artifacts and systems designs) dedicated to a given system type,
- Risks analysis grid template dedicated to a system type (may be presented in the form of questionnaires).

Note that this organization of the SALT framework contents and tools might be reorganized in the next period of the project, based on discussions internal to the consortium, on feedbacks following the real implantation of the tools, and on feedbacks from the use cases. The risk analysis template, described here as a matrix, is e.g. likely to be turned to a questionnaire, providing nevertheless the same type of outputs. A coherent description is proposed here in order to explain the coherence within the contents provided for the SALT framework.

The global coherence of the SALT contents is explained below:

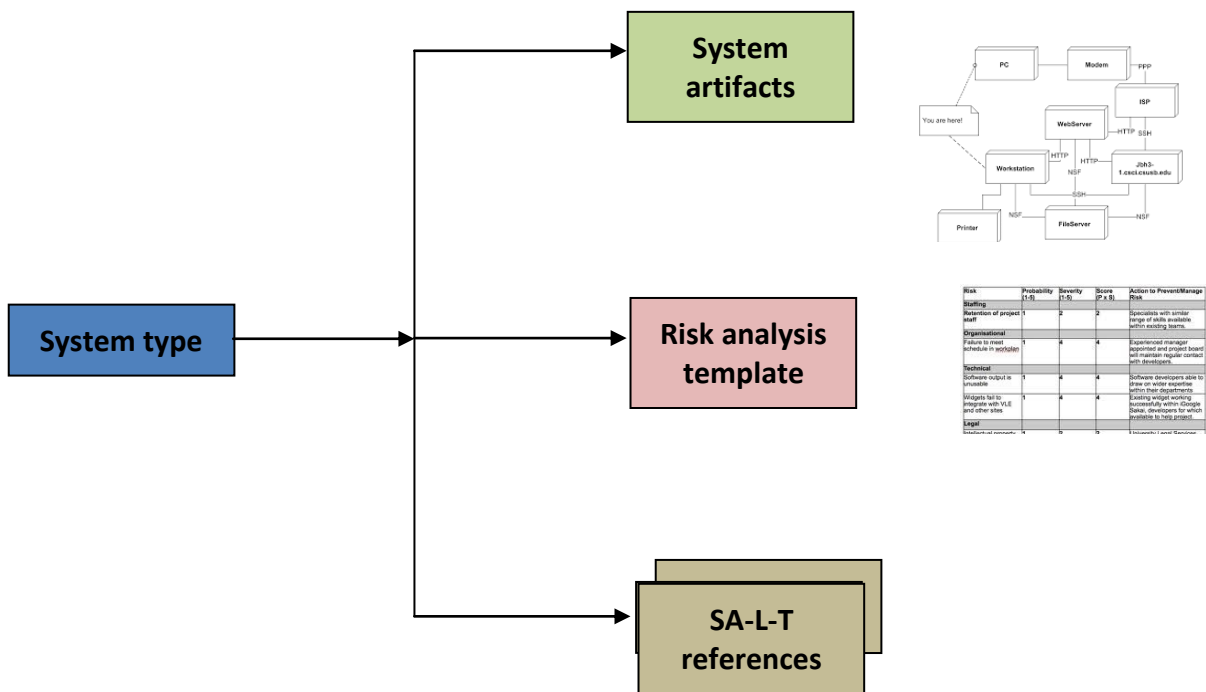


Figure 6: Internal contents of the SALT framework per system type

Examples of systems types are: video-surveillance system, biometric system.

The OCL rules embedded in some (if any) SALT references are applicable to the system design template (one or several) embedded within the system artifacts related to the system type.

Each new SALT project results in a SALT instance, which contains the references selected (manually) and therefore made applicable to the project/system of interest. This SALT reference, which remains modifiable, is itself recorded.

A SALT reference contains:

- The system type
- Information about the context of application,
- Legal and/or technical, and/or socio-ethical information organised in several SALT concerns.

A SALT reference context is made of several fields of information stating at least:

- The name of the SALT reference
- The country of application (potentially multiple)

Optionally a SALT reference also contains free fields of information enabling to ease the selection by the user. These fields contents can typically (but not restricted to) be based on the following examples:

- the 3 categories of concerns: Legal, Socio-Ethical, Technical,
- the 11 privacy principles from ISO/IEC 29100,
- the stage of application within the process: intention, conception, development, verification, deployment, use, maintenance; decommission.

For the record, the 11 privacy guidelines from ISO/IEC 29100 are:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information Security
11. Privacy compliance

A SALT concern is potentially reusable among several references, but all the SALT concerns within a given reference are to be applied as a whole, as they are coherent.

The figure below depicts an (non-definitive, as it is currently being updated) example of input interface for a SALT reference.

Reference 134

Version	1.0.0	Creator	Domingo Muñoz	<div style="display: flex; gap: 5px;"> <div style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">XML</div> <div style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">↓</div> </div>
Scope	Europe	Updated	2014-05-06 00:00:00	

Keywords
key1, key2, key3

Trust

Concerns

- Concern 1 [Principal]

Description
Description XX

Keywords
key1, key2

Rules

- IF true THEN false; ENDIF; (Error)
- WHILE true DO another thing; END (Info)

Figure 7: SALT reference example presentation for editing using the SFMT

A user of the SALT framework who wants to retrieve information for a given context of use (of a surveillance system) performs the interrogation of the SALT by specifying at least the context field selection (country of use and type of system), and optionally some keywords. Then the SFMT proposes him a list of references that matches. The user then has to manually browse and select the references he wants to apply to his system.

The diagram in Figure 8 below clarifies the general articulation of the different steps of the process of system development performed by the user and the integration of the SALT framework into the existing engineering process. It highlights how the selection of requirements and the SALT content can be integrated into standard development lifecycle.

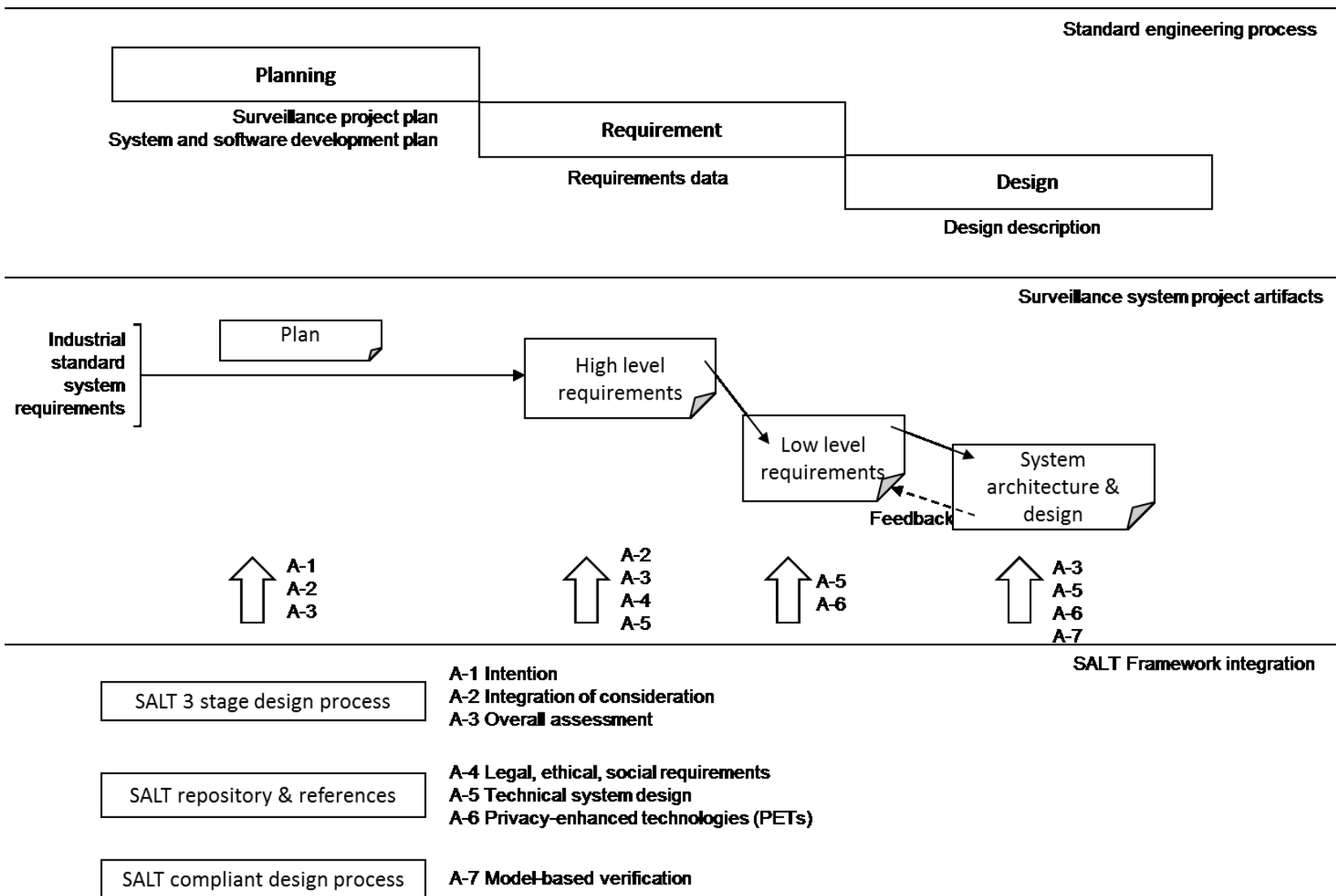


Figure 8: Integration of SALT framework to system development life cycle

The diagram is divided into three parts. It visualises conceptually, how the SALT framework can be integrated into surveillance system design.

1. Standard engineering process is common system development process, which often includes planning, requirement, and design, in waterfall as well as in V model. Note that we skip later phases such as implementation, integration, and testing etc., as Privacy by Design focuses on the early stage of the life cycle.

2. Surveillance system project artifacts. These are the artifacts produced during system development, which are visually aligned with the standard engineering process. Usually a surveillance project starts from existing industrial standards and baseline system requirements. The information will be further developed to create a plan suitable for both the client and technology provider and system integrator. High level requirements are specified in the requirement phase. These high level requirements need to be further specified or mapped to low level requirements, i.e. detailed technical requirements on surveillance system and its components (as well as subcomponents and functions). The process to identify and specify low level requirements might start at the requirement phase until design phase. Sometimes there is a feedback loop to modify the low level requirements during the system design. System architecture & design are artifacts that specify detailed system architecture and design.

3. SALT Framework integration illustrates how SALT framework is integrated into surveillance system development engineering process. The current SALT framework influences a surveillance system through three methods or processes: the 3 stage design process, the SALT repository with its collection of references, and the SALT compliant design process. These methods and processes connect the SALT framework to the system development.

Note that the diagram provides another perspective of the connection of the SALT framework and the use case, which is based on the same principle presented in other part of this document.

3.1.2 Correspondence with the 3 stage design process

The PARIS work-package 2 has defined a 3 stages process for the use of the SALT framework, as depicted within the figure below.

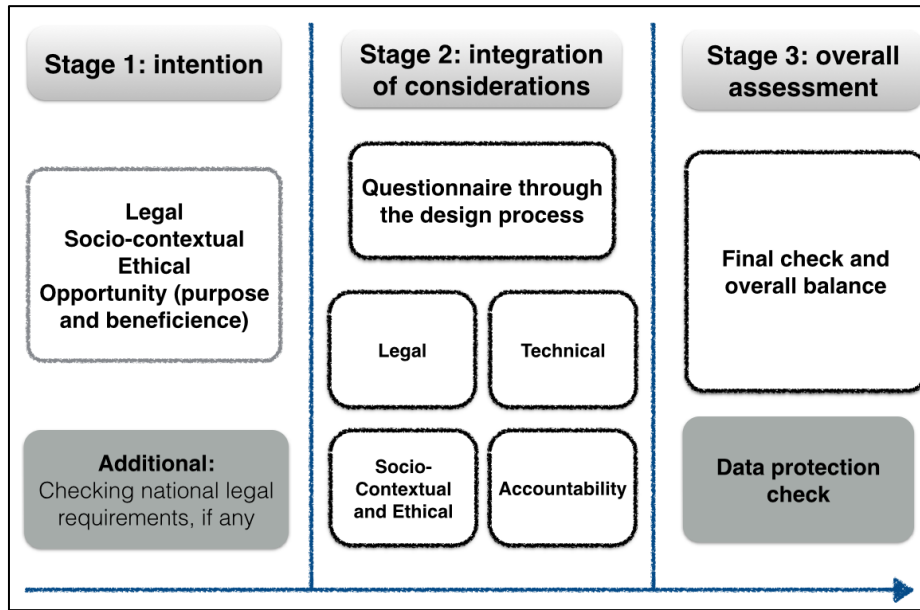


Figure 9: 3 stage process [from WP2]

The application of this 3-stage process is explained on the figure below, also with the distribution of the roles and actions among the stakeholders.

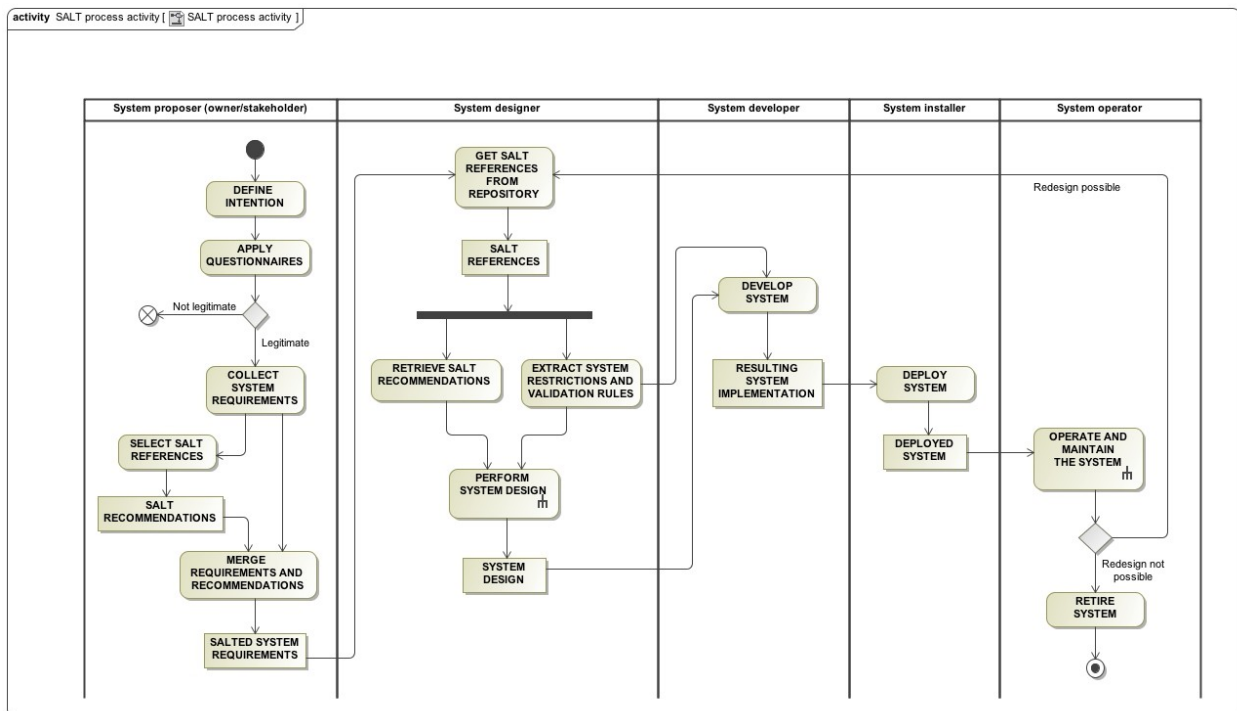


Figure 10: 3 stage process application using the SFMT

3.1.3 Specification of SALT references in this document

The SALT references within this document are presented as shown in the example below.

System type**Reference name****Context:** country**Context:** free fields**Concern 1 name****Concern 1 free fields**

Concern 1 contents

Concern 1 OCL rule

Concern 2 name**Concern 2 free fields**

Concern 2 contents

Concern 2 OCL rule

End

Moreover, the whole contents provided here are dedicated to video-surveillance systems, especially in France, which is the location chosen for the example application of the SALT processes and contents, mainly because it is one of the countries where the legal information about video-surveillance systems is most clearly formalized by law and the controlling authorities (the CNIL, which is the French DPA). It nevertheless causes needs to translate some existing legal texts, which is there performed partly, and without authorized translator, meaning that the arising contents are for research purposes mainly.

This language issue, especially regarding law texts, may point out the question of the mono-versus multi- language population of the SALT framework. At least it seems that even if some legal texts are translated for the sake of capability to mutually understand and compare approaches all over the European Union and wider, the end-reference might preferably be in native language. This issue shall be put in regard to the one about coexistence of different field of knowledge in the SALT approach (processes and contents) that raise some concerns because of by-mature difficulties of multi-disciplinary collaboration.

In the references proposed below in this document, some pieces of text are entirely extracted and pasted from external sources to the project, such as laws, publications. This is totally in line with the way the SALT framework and related tools are to be used, as they mainly are designed to aggregate existing information in a rationalized and searchable way rather than allowing creation of information.

3.2 Legal artifacts

3.2.1 Introduction to legal requirements about video-surveillance

The 2 use cases proposed here are focused on the use of video-surveillance by law enforcement authorities for investigation purposes. The use of images from video-surveillance cameras owned by public or private entities for investigation purposes by authorized law enforcement authorities is regulated with substantial differences between Member States. Indeed, such police access requests can be regulated under criminal law or criminal procedural legislations

(as in France), or under video-surveillance legislations (as in Belgium) or not regulated at all (as in the United Kingdom where access to images by LEA is mostly foreseen in a non-binding instrument).

In this document version, the goal is not to provide an exhaustive view of the SALT framework contents (especially here regarding Legal points in relation to video surveillance) for the use case, but to exhibit references that would be of interest for the context of the use case (Video Archive Search System used by Public authority and installed in public spaces). Some references out of the scope of the use case will also be exhibited, to allow demonstration of references manual selection by the end users (to show that not all the contents of the SALT Framework are applicable and that the selection of the references induces different constraints on the design of the system). The first articles of the French data protection Act are used as relative knowledge but only indirectly applicable to the use case. For example, article 1 of the French Data Protection Act defines the scope of application of the Act.

The references proposed below will all be stored in the SALT framework. They do not intend to be exhaustive.

Public/private balancing

The list of legal requirements that will act as constraints in the development and deployment of the technology subject of this use case are twofold:

- (1) Requirements that will frame the sharing of video footage by private or public operators with law enforcement authorities
- (2) Requirements that will define obligations for law enforcement authorities when processing the video footage for forensic purposes

In certain cases, the law provides that video surveillance systems may be installed for purposes related to the prevention of public order or prevention and investigation of crimes. In these cases, the access and use of video footage by LEA is therefore foreseen by law and even constitutes one of the main goals of the VS system. In other cases, the possibility given to law enforcement authorities to access images from video surveillance installed for private and unrelated purposes is derogation from the purpose specification principle. Such principle forbids further processing (such as sharing with third parties) for purposes not compatible with the original purpose of collection. The legislator has however foreseen derogations to the general principle when prevailing competing interests, such as the need for law enforcement to investigate criminal cases, justifies interference into individuals' privacy rights. In those cases, the balancing between public and private interests is made by the legislator who will define precisely the safeguards that should accompany the derogative regime. Such safeguards aim at reducing the impact on individuals' privacy.

Indeed, the rights to data protection and privacy are not absolute rights. Both of these rights are subject to limitations upon certain conditions, in particular, if they are provided by law.

The Data Protection Directive provides a list of conditions legitimizing the processing of personal data. According to the Directive, the processing of individual's (i.e. data subject's) personal data is lawful if unambiguous consent of the data subject is provided or if the processing of personal data is necessary in a particular situation. A particular situation may include the performance of a contract, compliance with a legal obligation, protection of the vital interests of the data subject, the performance of a task carried out in the public interest,

the exercise of official authority, and the legitimate interests of a controller.² This list should be read in the light of Recital 30 of Directive. According to the Directive the legitimate ground (i.e., interests of the data controller) should not override “the interests or the rights and freedoms of the data subject”. The Recital also foresees that in order “to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies”. In practice, national measures strike the balance between public and private interests can be challenged via lodging a complaint either to national data protection authorities or national courts.

Interferences into privacy by public authority are allowed if the test of legality, proportionality and legitimacy is performed. According to Article 8.2 of the ECHR “there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of other”.

The same trend has been approved in the recent United Nations General Assembly resolution 68/16719, which acknowledges that “the balancing of the interests involved in privacy and security, noting that public security may justify the gathering and protection of certain sensitive information, but States must ensure full compliance with their obligations under international human rights law”.

Contrary to the biometric use case (see D.6.2), the video surveillance use case actually lets little leeway to the different stakeholders to perform the balancing (through a privacy impact assessment). The legislator has already decided how the balancing should be made, since LEA access to images for specific law enforcement purposes is in general foreseen in national legislations. Still, this balancing provides for minimum requirements the system should meet. It is always possible to go beyond these requirements, and this is one of the goals of the PARIS project to incite stakeholders to implement strong privacy preserving requirements and practices.

3.2.2 Structure of legal references in this document

The use of the SALT methodology (once the system type is defined and selected) implies the selection of the applicable references. For this, it is proposed to prepare a basic questionnaire focusing on some essential contextual elements that will allow identifying under which legal texts and scope of application the intended system falls.

The challenge here is to extract essential criteria from the scope of application of legal norms in order to support the user in identifying the relevant legal references that should be taken into account.

A legal reference contains:

² Directive 95/46/EC, Article 7.

- The system type to which the legal reference applies. A legal reference may indeed be found to apply to specific technologies (video surveillance), data controllers (e.g. Law enforcement authorities), or purposes of use of the system (criminal investigations), or to be broadly applicable to a personal data processing activity.

A SALT reference context is made of several fields of information based on the criteria used by the law to define its scope of application, stating at least:

- The name of the SALT reference, which is basically the formal/official name of the legal norm in question (e.g. code of criminal procedure, law on video surveillance...)
- A first layer of context information, which will define the territorial scope of application (EU, France, Flanders)
- Additional layers of information based on the criteria used to define the material scope of application of the law. As a way of example:
 - French law contains different rules applicable to the place monitored by the video surveillance system. It follows that a given system type (video surveillance) might actually be submitted to different regimes, according to whether cameras monitor public spaces, or publicly accessible premises or non-publicly accessible premises (see example *Infra*). The SALT framework will thus indicate as second layer: public space/publicly accessible premises/ non publicly accessible premises.
 - The Law Enforcement data Protection Directive uses two criteria to define its material scope of application (each of them requiring a layer of context information):
 - identity of the data controller: the Directive only applies to law enforcement authorities as defined in the Directive
 - purpose of the processing: prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
- Where necessary and relevant a final layer of context information may be provided: following our example of classification of spaces in the case of video surveillance, the SALT framework may provide examples of contexts in which the legal reference applies (shops, banks, etc.)

Concerns are used to **specify the legal requirement** that is stated under the said legal reference.

3.2.3 Table of proposed legal references in this document

As explained above, the goal of this document is not to be fully exhaustive, but rather to provide examples of SALT references. Nevertheless, as the goal is, in future works and in the next deliverables, to demonstrate and test the SALT approach and tools on 2 use cases (those described in the first part of this document), the table below sums up the legal references described in the next document section, and proposes a classification for its use within the following possibilities:

- May be applicable to use-case 1 (privacy preserving law enforcement to video archive search)
- May be applicable to use case 2 (accountability of video-surveillance operators)
- Rather provided as SALT example contents.

This classification remains nevertheless performed in an indicative and illustrative way, as the process of building a SALT instance for a given context (by the selection of the applicable references to the context) remains to be done on a case-by-case basis by the users of the SALT tools and cannot be at all considered as unique for this context. Indeed, if certain legal references are binding rules and should therefore be selected where they will find to apply to a given system, other legal references are non-binding (example: regulation proposal and directive proposal under discussion, recommendations issued by supervisory authorities, norm ISO, etc.) and will not have to be taken into account in all cases. In that perspective, another user or team of users may consider different choices. Nevertheless, the “strength” of the applicability of a reference will vary: some of them are very likely to be selected, other appear as less likely. This is depicted in the table as specified below:

- *** reference highly likely to be selected within the use case context,
- ** reference likely to be selected within the use case context,
- * reference less likely to be selected within the use-case context

References description. Fields	References descriptions	Applicability to use-case 1	Applicability to use-case 2	Example
Reference name	Belgium Law on video-surveillance 2007 (amended 2009)			***
System type	video-surveillance systems			
Context	Belgium			
Reference name	Information Commissioner's CCTV Code of Practice			***
System type	video-surveillance systems			
Context	United Kingdom			
Reference name	French homeland security code - video-surveillance in public spaces	**	**	***
System type	video-surveillance systems			
Context	France			
Reference name	French homeland security code - video-surveillance in publicly accessible premises	**	***	***
System type	video-surveillance systems			
Context	France			
Reference name	French homeland security code – Fight against terrorism - video surveillance			***
System type	Video-surveillance systems			
Context	France			
Reference name	technical requirements from French ministerial decree of 3 August 2007	***	**	***
System type	Video-surveillance systems			
Context	France			
Reference name	French Code of Criminal Procedure - (art. 60-1, 77-1-1, 93-3)	***	*	***
System type	All			
Context	France			
Reference name	French Data Protection Act (Act n°78-17 of 6 January 1978)	*	**	***
System type	All surveillance systems			
Context	EU			
Reference name	EU Law Enforcement Data Protection Directive Proposal (pending legislative act – not approved)	*	**	***
System type	All			
Context	EU			
Reference name	EU data Protection Regulation Proposal (not approved yet)			

System type	All surveillance systems	*	**	***
Context	EU			

Table 1: applicability of Legal SALT references to the WP5 Use-Cases

This classification is also based on the hypothesis that the location chosen for the use cases demonstrations (and selected through the SALT management tools) is France. This choice is performed because of the existence of a large and accessible corpus of laws and recommendations about video-surveillance in this country.

3.2.4 Access to images by law enforcement authorities in Belgium

System type	video-surveillance systems
Reference name	Belgium Law on Video surveillance 2007 (amended 2009)
Context:	Belgium
Context:	video surveillance in public spaces, video surveillance in publicly accessible premises
Context: free fields	public roads, market places, streets, squares, parks, shops, banks, restaurants, cafés, cinema
Concern 1 name	Access request by law enforcement authorities
Concern 1 add. Fields	data sharing, disclosure

Concern 1 contents

- The controller **can** (the person responsible of the video-surveillance system) transmit the images to police services or judicial authorities if he observes breaches of the law or nuisances and the images are likely to have an evidential value or can contribute to identify the authors.³
- The controller **shall** transmit, free of charge, the images to police authorities acting in the course of their missions of administrative police or judicial police on their request.

Concern 1 OCL rule **NONE**

Concern 2 name	Access requests by law enforcement authorities
Concern 2 add. Fields	data sharing, disclosure

Concern 2 contents

- The controller **can** transmit the images to police services or judicial authorities if he observes breaches of the law or nuisances and the images are likely to have an evidential value or can contribute to identify the authors.
- The controller **must** transmit, free of charge, the images to police authorities acting in the course of their missions of judicial police, on presentation of a judicial warrant.⁴

³ Article 9 1° of the law on video surveillance

⁴ Article 9 2° of the law on video surveillance

Concern 2 OCL rule **NONE**

end

3.2.5 Access to image by public forces for investigation purposes in United Kingdom

System type	video-surveillance systems
Reference name	Information Commissioner's CCTV Code of Practice
Context:	United Kingdom
Context: free fields	NA
Concern 1 name	Access to images
Concern 1 add. Fields	disclosure, data sharing

Concern 1 contents

Recorded material should be stored in a way that maintains the integrity of the image. This is to ensure that [...] the material can be used as evidence in court. To do this you need to carefully choose the medium on which the images are stored, and then ensure that access is restricted. You may wish to keep a record of how the images are handled if they are likely to be used as evidence in court. Finally, once there is no reason to retain the recorded images, they should be deleted."

"Many modern CCTV systems rely on digital recording technology and these new methods present their own problems. With video tapes it was very easy to remove a tape and give it to the law enforcement agencies such as the police for use as part of an investigation. It is important that your images can be used by appropriate law enforcement agencies if this is envisaged. If they cannot, this may undermine the purpose for undertaking CCTV surveillance."

"Disclosure of images from the CCTV system must also be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet."

Images can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.

NOTE: Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime."

"Judgements about disclosure should be made by the organisation operating the CCTV system. They have discretion to refuse any request for information unless there is an overriding legal

obligation such as a court order or information access rights. Once you have disclosed an image to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with the Data Protection Act (DPA) in relation to any further disclosures.

The method of disclosing images should be secure to ensure they are only seen by the intended recipient.”

Concern 1 OCL rule **NONE**

end

3.2.6 Video surveillance in France

The regulation of video surveillance in France mainly follows from two laws. The Act on Information Technologies and Civil Liberties ('Loi Informatique et Libertés')⁵ is mainly applicable to cameras monitoring *non publicly accessible spaces*. The monitoring of *publicly accessible spaces/premises* by means of cameras is regulated by the 'Loi d'orientation et de programmation pour la sécurité intérieure'⁶ as amended, the provisions of which can now be found in the Homeland security code. The French "code de la securite intérieure" is a French law created in 2012 to group all the laws and regulations about homeland security. Some essential statements about video-surveillance in French law are therefore embedded in this text. Further technical specifications regarding cameras submitted to the scope of application of the Homeland security Code are provided via ministerial decree ("Arrêté de 2007"), which is therefore another highly relevant source of law to take into account for the installation of cameras. Finally, other relevant legislations may be retrieved thanks to the SALT framework, such as the conditions for access to images by police authorities, which are actually provided under the Code of Criminal Procedure (and not under the Homeland security Code or Information Technologies and Civil Liberties Act).

An essential aspect of the SALT framework will consist in identifying the relevant legal instrument applicable to a certain type of video surveillance. For this, an essential criterion to be taken into account is the type of places monitored (public space, publicly accessible premise or non-publicly accessible premises). Such criteria will need to be refined. The information below is destined to provide a first overview of the variety of legal requirements/information that may be extracted from the SALT framework.

3.2.6.1 French Homeland security Code

System type	Video-surveillance system
Reference name	French Homeland security code - video-surveillance in public spaces
Context 1:	France
Context 2:	Video surveillance of public spaces

⁵ Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties – Loi No. 78-17 Informatique et Libertés du 6 Janvier 1978 – as amended

⁶ Act No. 95-73 of 21 January 1995 on homeland security orientation and programming - Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation pour la sécurité intérieure

Context: free fields	Parks, streets, public roads, open markets, high ways
Concern 1 name	article L251-1 and following (partial)
Concern 1 add. Fields	Legal, intention, Purpose legitimacy and specification

Concern 1 contents

The transmission and the recording of images from video cameras monitoring public spaces (“voie publique”), can be implemented by the competent public authorities for the following purposes:

- 1) Protection of buildings and public installations and nearby;
- 2) Safeguard of national defence installations;
- 3) Regulation of transportation flows;
- 4) Detection of road traffic offences;
- 5) Prevention of offences against people or goods;
- 6) Prevention of terrorist acts according to article L223-1 and following of the Homeland security Code;
- 7) Prevention of natural or technological disasters;
- 8) Emergency assistance to individuals and fire protection;
- 9) Safety of installations in amusement parks.

Concern 1 OCL rule **NONE**

end

System type	Video-surveillance systems
Reference name	French Homeland security code - video-surveillance in publicly accessible premises
Context 1:	France
Context 2:	Video surveillance of publicly accessible premises
Context: free fields	Banks, shopping mall, cinemas
Concern 1 name	article L251-1 and following (partial)
Concern 1 add. Fields	Legal, intention, Purpose legitimacy and specification

Concern 1 contents

Regarding publicly accessible premises (whether public or private premises), video surveillance may be installed to ensure the security of people and goods where these premises are particularly exposed to risks of aggression or theft.

They can also be installed when subject to terrorist threats (see Ref. Homeland security Code – Fight against terrorism – video surveillance)

Concern 1 OCL rule **NONE**

Concern 2 name (partial)	article L252-5, maximum duration of video-footages retention
Concern 2 add. Fields	Legal, intention, Purpose legitimacy and specification

Concern 2 contents

Except in the case of flagrante delicto, or judiciary preliminary investigation, video-surveillance recordings are erased within an authorized maximum amount of time. This amount of time can never exceed 1 month.

[...]

Concern 2 OCL rule **NONE**

end

System type	Video-surveillance system
Reference name	French homeland security code – Fight against terrorism - video surveillance
Context:	France
Context:	Public spaces, publicly accessible premises
Context: free fields	
Concern 1 name	article L223-1 and following (partial)
Concern 1 add. Fields	Legal, intention, Purpose legitimacy and specification

Concern 1 contents

[...]

Concern 1 OCL rule **NONE**

3.2.6.2 Ministerial decree of 3 August 2007 and its technical annex

The first reference below is obtained as a translation of the abovementioned legal text. Please note that the translation has not been realized by a certified translator, meaning that the reference for its extensive use shall be the French original text.

Moreover, in this document version, the reference is not complete. The goal is to explain and illustrate the key concepts underlying under a SALT reference.

System type	Video-surveillance system
Reference name	technical requirements from French ministerial decree of 3 August 2007
Context:	France
Context	video surveillance in public spaces, video surveillance in publicly accessible spaces
Context: free fields	parks, public roads, streets, restaurants, cafés, cinemas, shopping mall
Concern 1 name	data minimisation, orientation of cameras
Concern 1 add. Fields	

Concern 1 contents

Article 1:

The data controller has to ensure that the cameras are tuned, equipped and connected in such a way that the images made available in real time of post-processing enable to reach the security objective for which the system has been installed.

Limiting orientation of video equipment to a particular perspective can ensure that data controller collects only necessary data for the performance of the system. Limiting orientation of video equipment could also ensure that data that is collected is not too excessive for the specified purposes. For example, cameras could be positioned in a way that would not capture the images of persons not visiting premises.

The first consequence is that the objectives of the system are to be stated on a per-camera basis. This requirement hangs over each camera and over the whole system.

[...]The second consequence is that the technical features of the cameras shall enable to reach the goals of the system.

[...]

Concern 1 OCL rule **NONE**

Concern 2 name **Data sharing: technical requirements**

Concern 2 add. Fields

Concern 2 contents

The exportation of images (sharing with law enforcement authorities) from systems of video surveillance is subject to technical requirements:

- Surveillance cameras with narrow fields of view shall have a format greater than or equal to 704 x 576 pixels.
- Other cameras with wide fields of view (and notably those monitoring traffic roads) shall have a format greater than or equal to 352 x 288 pixels.
- A minimum of 12 images per second for cameras with narrow fields of view
- A minimum of 6 images per second for other cameras with wide fields of view
- All operations of exportations must be logged: list of flows of images exported, date and time of images, duration, identification of cameras concerned, date and time of exportations, identity of the person carrying out the exportation
- Images are exported without reduction of the image's quality. If the exportation of the images requires to modify their format, the compression of the images should not undermine their quality
- The video surveillance system must continue to record during the operation of exportation
- The images exported are stocked on a non-rewritable system (in general they will be burned or a CD or DVD). USB key, as rewritable system, are not allowed. The use of a hard drive is only allowed when an important quantity of images must be exported.
- The software to exploit the images must also be transmitted to the police. It must allow:
 - o To read the records without reduction of images' quality
 - o To read the records over cranking and under cranking
 - o To read image by image

- To know the identification of the camera, date and time of the record
- To search by camera, date and time
- [the table below is directly extracted from the French law, it shall be translated and also only the cases dedicated to public spaces shall be retained]
-

SITUATION	RÉSOLUTION minimum de l'image stockée	NOMBRE D'IMAGES par seconde au minimum	COMMENTAIRES classification plan étroit/plan large
Caméra de surveillance de la voie publique en agglomération aux abords d'un site sensible.	CIF	6	Plan large.
Caméra de surveillance d'un monument sur la voie publique	CIF	6	Plan large.
Caméra de surveillance d'un automate (DAB...).	4 CIF*	6	Plan étroit.
Caméra de surveillance à l'intérieur d'un véhicule de transport public.	4 CIF*	6	Plan étroit.
Caméra de surveillance sur un quai de gare.	CIF	6	Plan large.
Caméra de surveillance en entrée ou sortie d'un commerce, d'un musée, d'une agence bancaire, d'un lieu ouvert au public.	4 CIF*	12 ou 6	Plan étroit 6 si un dispositif de filtrage des flux de personnes est présent (sas, toumiquet...).
Caméra de régulation du trafic routier	CIF	6	Plan large.
Caméra de surveillance d'un comptoir ou d'un guichet.	4 CIF	6	Plan large.
Caméra de surveillance de rayons d'un magasin.	CIF	6	Plan large.
Caméra de surveillance d'une pompe de carburant.	4 CIF*	6	Plan étroit.
Caméra de surveillance d'une caisse ou d'un terminal de paiement.	4 CIF*	6	Plan étroit.

Concern 2 OCL rule : several rules, embedding all possible constraints from the concern

end

3.2.6.3 Code of Criminal Procedure

System type	All
Reference name	French Code of Criminal Procedure - (art. 60-1, 77-1-1, 93-3)
Context:	France
Context: free fields	image data, documents, computer files, and other data
Concern 1 name	Access to images by law enforcement agencies
Concern 1 add. Fields	Disclosure legitimacy, purpose

Concern 1 contents

Access to images is limited to activities of judicial police for the purposes of investigation of crimes and offences sentenced by imprisonment.

Concern 1 OCL rule NONE

Concern 2 name	Obligation to transmit evidence to law enforcement authorities
Concern 2 add. Fields	Legitimate ground, purpose

Concern 2 contents

Obligation for any person, public or private entity or public administration susceptible to be in possession of documents of interest for an on-going criminal investigation, including documents issued from a computer based system, to transmit these documents to the police. Failure to satisfy this obligation is punished by a fine of 3750 euros.

Concern 2 OCL rule **NONE**

3.2.6.4 France - French Data Protection Act (Act n°78-17 of 6 January 1978)

This use case should also consider the constraints put by the Law on operators of video surveillance systems whose access is requested.

Under French Law, these operators are subject to the general Information Technologies and Civil Liberties Act when installing a video surveillance system monitoring non publicly accessible premises, such as offices or private premises. However, it must be underlined that the IT and Civil Liberties Act has a wide scope of application and is not limited to video surveillance system.

We extract only the requirements specific to the sharing of the images with third parties and more general requirements with regard to accountability and security.

System type	All
Reference name	French Data Protection Act (Act n°78-17 of 6 January 1978)
Context:	France
Context: free fields	NA
Concern 1 name	Legitimacy
Concern 1 add. Fields	legitimate ground for processing personal data

Concern 1 contents

The processing of personal data must have received the consent of the data subject or must meet one of the following conditions:

1° compliance with any legal obligation to which the data controller is subject;

2° the protection of the data subject's life;

3° the performance of a public service mission entrusted to the data controller or the data recipient;

4° the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract;

5° the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.

There is an obligation stemming from the French Criminal Procedure Code for operators to share the information requested by Law enforcement authorities within criminal and judicial investigations.

It is recommended that the Privacy Management Program/internal privacy policy should indicate practices and policies which would allow accommodating requests made by the LEA. As part of these practices and policies, the controller should ensure data minimization principle and security of personal data that has been forwarded upon the request of the LEA.

Concern 2 name **Accountability: Data protection officer**

Concern 2 add. Fields **Appointment and role**

Concern 2 contents

A data controller may appoint a personal data protection officer (“Correspondant à la protection des données personnelles”) charged with ensuring, in an independent manner, compliance with the obligations provided for in the Data Protection Act.

A data protection officer is responsible for overseeing the organization’s compliance with applicable privacy legislation. It should be noted that an organization remains accountable for compliance with applicable privacy legislation. Appointing an individual to be responsible for the program does not negate the organization’s accountability.

The appointment of the officer shall be notified to the «Commission Nationale de l’Informatique et des Libertés (French Data Protection Authority). It shall be brought to the attention of the employee representative bodies.

The officer shall be a person who shall have the qualifications required to perform his duties. He shall keep a list of the processing carried out, which is immediately accessible to any person applying for access, and may not be sanctioned by his employer as a result of performing his duties. He may apply to the «Commission Nationale de l’Informatique et des Libertés” when he/she encounters difficulties in the performance of his duties.

Concern 2 OCL rule **NONE**

Concern 3 name **Security**

Concern 3 add. Fields

Concern 3 contents

The data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties (Art. 34).

Concern 3 OCL rule **NONE**

Concern 4 name **Entities competent to create forensic systems**

Concern 4 add. Fields

Concern 4 contents

Processing of personal data relating to offences, convictions and security measures may be put in place only by (art. 9):

1°the courts, public authorities and legal entities that manage public services, within the framework of their legal remit;

2°the representatives of the law for the strict needs of the exercise of the functions granted to them by the law;

3° [Provisions considered contrary to the Constitution by decision No. 2004-499 DC of 29 July 2004 of the Constitutional Court];

4° the legal persons mentioned in Articles L321-1 and L331-1 of the Intellectual Property Code, acting by virtue of the rights that they administer or on behalf of victims of infringements of the rights provided for in Books I, II and III of the same Code, and for the purposes of ensuring the defence of these rights.

This article means that only the entities mentioned can act as controller. It does not prevent other entities to act as data processors (acting under the instructions of the data controller)

Concern 4 OCL rule **NONE**

Concern 5 name **Authorisation**

Concern 5 add. Fields

Concern 5 contents

An order of the competent Minister or Ministers shall authorise, after a reasoned and published opinion of the CNIL, the processing of personal data carried out on behalf of the State and whose purpose is the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures. The opinion of the Commission shall be published together with the order authorising the processing. (Art. 26)

Concern 5 OCL rule **NONE**

Concern 6 name **Data subject rights**

Concern 6 add. Fields policies, procedures

Concern 6 contents

The Privacy Management Program/internal privacy policy should indicate practices and policies which would allow ensuring that the controller knows how to respond to individuals making access requests for copies of their own images or seeking to exercise their rights to rectification or erasure.

Concern 6 OCL rule **NONE**

end

3.2.7 Law Enforcement Data Protection Directive

The European Commission has proposed a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. This Directive aims at harmonising the

level of protection of the rights and freedoms of individuals with regard to the processing of personal data by law enforcement authorities within criminal investigations. This is seen as a requirement for facilitating the free flow of information between law enforcement agencies within the European Union.

This proposal for a Directive is of interest for our use case in so far as it further specifies accountability measures. In particular, the proposal for the Directive specifies requirements for documentation and keeping of records. Once the Directive is adopted the Member States of the EU would have to make sure that domestic legislations would require the LEA to 1) document: (a) the name and contact details of the controller, or any joint controller or processor; (b) the purposes of the processing; (c) the recipients or categories of recipients of the personal data; (d) transfers of data to a third country or an international organisation, including the identification of that third country or international organization and 2) to keep records of “at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure”. The proposal for the Directive foresees that the LEA 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”.

The processing of video footage by European law enforcement agencies for forensic purposes within criminal investigations will fall under the provision of this Directive.

We extract from this text the requirements that will apply to the use case.

System type	All
Reference name	EU Law Enforcement Data Protection Directive Proposal (pending legislative act – not approved)
Context 1:	EU
Context 2:	Processing activities by national law enforcement authorities
Context 3:	Prevention, investigation, detection or prosecution of criminal investigations
Context: free fields	None
Concern 1 name	Article 4 a) Concern 1 add. Fields
Concern 1 add. Fields	Legitimate ground, purpose

Concern 1 contents

Personal data must be processed lawfully (art. 4(a)).

Data processing activities are deemed lawful only if and to the extent that the processing is based on a law and is necessary (Art. 7.1):

- (a) For the performance of a task carried out by a competent authority; or
- (b) For compliance with a legal obligation to which the controller is subject; or
- (c) In order to protect the vital interests of the data subject or of another person; or
- (c) In order to protect the vital interests of the data subject or of another person; or
- (d) For the prevention of an immediate and serious threat to public security.

Concern 1 OCL rule **NONE**

Concern 2 name **Article 4**

Concern 2 add. Fields **Access to third parties' video surveillance systems,**
Legitimate ground, purpose

Concern 2 contents

Law enforcement authorities may only have access to personal data initially processed for purposes other than those of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, if they are specially authorised by a law.

The law enforcement agency, before requiring access to third party's video surveillance system should ensure it has sufficient legal basis to do so. (Article 4 a)

Concern 2 OCL rule **NONE**

Concern 3 name **Article 4a 1c**

Concern 3 add. Fields **Access to third parties' video surveillance systems** Request for access

Concern 3 contents

Request for access must be in writing and refer to the legal ground for the request (article 4a 1a). The written request must be documented

Concern 3 OCL rule **NONE**

Concern 4 name **Article 4**
Concern 4 add. Fields **Access to third parties' video surveillance systems,**
Access to the data

Concern 4 contents

Access is allowed only by duly authorised staff of the law enforcement authority in the performance of their task where, in a specific case, reasonable grounds give reason to believe that the processing of the personal data will substantially contribute to the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties

Concern 4 OCL rule **NONE**

Concern 5 name **Article 4**

Concern 5 add. Fields **Data retention, Deletion**

Concern 5 contents

Personal data should be deleted by law enforcement authorities when they are no longer necessary for the purposes for which they were processed.

Concern 5 OCL rule **NONE**

Concern 6 name **Article 4**

Concern 6 add. Fields **Data retention, Deletion, accountability, data quality**

Concern 6 contents

Law enforcement authorities should put mechanisms in place to ensure that time limits are established for the erasure of personal data. (art. 4b)

Law enforcement authorities should put mechanisms in place to ensure a periodic review of the need for the storage of the data, including fixing storage period for the different categories of data. (art. 4b)

Procedural mechanisms should be established to ensure that those time-limits or the periodic reviews intervals are observed. (art. 4b)

Concern 6 OCL rule **NONE**

Concern 7 name **Article 5. 1**

Concern 7 add. Fields **Categorisation of data, data quality**

Concern 7 contents

Data controllers should make a clear distinction between the following categories of data subjects:

- (a) Persons with regard to whom there are reasonable grounds for believing that they have committed or are about to commit a criminal offence
- (b) Persons convicted of a crime
- (c) Victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence
- (d) Third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceeding, or a person who can provide information on criminal offences, or a contact or associate to the one of the persons mentioned in (a) or (b)
- (e) other

Concern 7 OCL rule **NONE**

Concern 8 name **Article 5**

Concern 8 add. Fields **Categorisation of data, data quality**

Concern 8 contents

Processing of data of other data subjects than the ones mentioned in art. 5.1 may only be processed:

(a) as long as necessary for the investigation or prosecution of a specific criminal offence in order to assess the relevance of the data for one of the categories indicated in paragraph 1; or

(b) When such processing is indispensable for targeted, preventive purposes or for the purposes of criminal analysis, if and as long as this purpose is legitimate, well defined and specific and the processing is strictly limited to assess the relevance of the data for one of the categories indicated in art.5.1 this is subject to regular review at least every six months. Any further use is prohibited.

Concern 8 OCL rule **NONE**

Concern 9 name **Article 6.1**

Concern 9 add. Fields **Accuracy and reliability of personal data, data quality, accuracy**

Concern 9 contents

The accuracy and reliability of personal data undergoing processing should be ensured.

Concern 9 OCL rule **NONE**

Concern 10 name **Article 6.2**

Concern 10 add. Fields **categorisation of data, data quality, accuracy**

Concern 10 contents

Personal data based on facts should be distinguished from personal data based on assessments, in accordance with their degree of accuracy and reliability.

Concern 10 OCL rule **NONE**

Concern 11 name **Article 8**

Concern 11 add. Fields **categorisation of data, specific categories of data**

Concern 11 contents

Personal data revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of biometric data or data concerning health or sex life is prohibited. (art. 8.1)

Exceptions (art. 8.2):

(a) The processing is strictly necessary and proportionate for the performance of a task carried out by law enforcement authorities on the basis a law; or

(b) The processing is necessary to protect the vital interests of the data subject or of another person; or

(c) The processing relates to data which are manifestly made public by the data subject, provided that they are relevant and strictly necessary for the purpose pursued in a specific case.

Concern 11 OCL rule **NONE**

Concern 12 name	Article 6.3	Concern 12 add. Fields	Data sharing, data quality, accuracy
------------------------	--------------------	-------------------------------	---

Concern 12 contents

Personal data which are inaccurate, incomplete or no longer up to date should be transmitted or made available. To this end, law enforcement authorities shall assess the quality of personal data before they are transmitted or made available. (Art. 6.3)

As far as possible, in all transmissions of data, available information shall be added which enables the receiving law enforcement authority to assess the degree of accuracy, completeness, up-to-dateness and reliability. (Art. 6.3)

Personal data shall not be transmitted without request from a competent authority, in particular data originally held by private parties.

Concern 12 OCL rule	NONE
----------------------------	-------------

Concern 13 name	Article 6.4
Concern 13 add. Fields	Data sharing, Sharing of incorrect data, unlawful sharing

Concern 13 contents

If it emerges that incorrect data have been transmitted or data have been transmitted unlawfully, the recipient must be notified without delay.

The recipient shall be obliged to rectify the data without delay or to erase them in accordance.

Concern 13 OCL rule	NONE
----------------------------	-------------

Concern 14 name	Art. 55
Concern 14 add. Fields	Data sharing, Transmission of personal data to other parties

Concern 14 contents

The controller should not transmit or instruct the processor to transmit personal data to A natural or legal person not subject to the provisions adopted pursuant to this Directive (law enforcement authorities processing personal data for the purpose of criminal investigations), unless (Art. 55 a):

- (a) The transmission complies with Union or national law; and
- (b) The recipient is established in a Member State of the European Union; and
- (c) No legitimate specific interests of the data subject prevent transmission; and
- (d) The transmission is necessary in a specific case for the controller transmitting the personal data for:
 - (i) The performance of a task lawfully assigned to it; or
 - (ii) The prevention of an immediate and serious danger to public security; or
 - (iii) The prevention of serious harm to the rights of individuals.

The controller shall inform:

- the recipient of the purpose for which the personal data may exclusively be processed
- the supervisory authority of such transmissions

- The recipient of processing restrictions and ensure that these restrictions are met.

Concern 14 OCL rule **NONE**

Concern 14 name **Article 6.3**
Concern 15 add. Fields **Data sharing, requirement for sharing**

Concern 15 contents

Personal data shall not be transmitted without request from a competent authority, in particular data originally held by private parties. (Art. 6.3)

Concern 15 OCL rule **NONE**

Concern 16 name **Article 4 f)**
Concern 16 add. Fields **Accountability, Legitimate ground, purpose, accountability**

Concern 16 contents

Personal data must be processed under the responsibility and liability of the controller, who shall ensure and be able to demonstrate compliance with the legal framework.

The controller must document requests for access to images contained in third party's video surveillance systems and link this information to such images in the database.

Concern 16 OCL rule **NONE**

Concern 17 name **Article 7a 1**
Concern 17 add. Fields **Further processing, legitimate ground, purpose**

Concern 17 contents

Personal data may only be further processed for another purpose which is not compatible with the purposes for which the data were initially collected (by the law enforcement authority) if and to the extent that (art. 7a 1):

- The purpose is strictly necessary and proportionate in a democratic society and required by law for a legitimate, well-defined and specific purpose;
- The processing is strictly limited to a period not exceeding the time needed for the specific data processing operation.

Concern 17 OCL rule **NONE**

Concern 18 name **Articles 9 and 10**
Concern 18 add. Fields **Rights of data subjects**

Concern 18 contents

The controller should have concise, transparent, clear and easily accessible policies with regard to the processing of personal data and for the exercise of the data subject's rights: right to the provision of clear and understandable information, right of access, rectification and erasure, right to obtain data, right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from unlawful processing operation.

Such rights shall in general be exercised free of charge.

The data controller shall respond to requests from the data subject within a reasonable period of time.

Concern 18 OCL rule **NONE**

Concern 19 name **Article 31 2c)**

Concern 19 add. Fields **Rights of data subjects, contact with the DPO**

Concern 19 contents

Data subjects have the right to contact the data protection officer on all issues related to the processing of his or her personal data.

Concern 19 OCL rule **NONE**

Concern 20 name **Article 18**

Concern 20 add. Fields **Accountability, demonstration of compliance**

Concern 20 contents

The controller adopts policies and implements appropriate measures to ensure and be able to demonstrate, in a transparent manner, for each processing operation, that the processing of personal data is performed in compliance with the data protection framework, both at the time of the determination of the means for processing and at the time of the processing itself. (Art. 18)

This obligation includes:

- (a) Keeping the documentation referred to in Article 23 [link to article or reference about art. 23];
- (a) Performing a data protection impact assessment pursuant to Article 25a [link to article or reference about art. 25a]
- (b) Complying with the requirements for prior consultation pursuant to Article 26 [link to article or reference about art. 26]
- (c) Implementing the data security requirements laid down in Article 27 [link to article or reference about art. 27]
- (d) Designating a data protection officer pursuant to Article 30; [link to article or reference about art. 30]
- (e) Drawing up and implementing specific safeguards in respect of the treatment of personal data relating to children, where appropriate

The controller shall implement mechanisms to ensure the verification of the adequacy and effectiveness of the measures referred above. If proportionate, this verification shall be carried out by independent internal or external auditors.

Concern 20 OCL rule **NONE**

Concern 21 name **Article 23**

Concern 21 add. Fields **Accountability:** documentation

Concern 21 contents

Each controller and processor should maintain documentation of all processing systems and procedures under their responsibility.

The documentation shall contain at least the following information:

- (a) The name and contact details of the controller, or any joint controller or processor;
 - (aa) A legally binding agreement, where there are joint controllers; a list of processors and activities carried out by processors;
- (b) The purposes of the processing;
 - (ba) An indication of the parts of the controller's or processor's organisation entrusted with the processing of personal data for a particular purpose;
 - (bb) A description of the category or categories of data subjects and of the data or categories of data relating to them
- (c) The recipients or categories of recipients of the personal data;
 - (ca) Where applicable, information about the existence of profiling, of measures based on profiling, and of mechanisms to object to profiling;
 - (cb) Intelligible information about the logic involved in any automated processing;
- (d) Transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and the legal grounds on which the data are transferred; a substantive explanation shall be given when a transfer is based on Articles 35 or 36 of this Directive;
 - (da) The time limits for erasure of the different categories of data;
 - (db) The results of the verifications of the measures referred to in Article 18(1);
 - (dc) An indication of the legal basis of the processing operation for which the data are intended.

The controller and the processor shall make all documentation available, on request, to the supervisory authority.

Concern 21 OCL rule **NONE**

Concern 22 name **Article 24**

Concern 22 add. Fields **Accountability:** keeping of records

Concern 22 contents

Records should be kept of at least the following 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,
- 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 purposes of auditing, either by the data protection officer or by the data protection authority.

The controller and the processor shall make the records available, on request, to the supervisory authority.

Concern 22 OCL rule **NONE**

Concern 23 name **Article 30**

Concern 23 add. Fields **Accountability: Data protection officer**

Concern 23 contents

The controller or the processor should designate a data protection officer.

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32 [link to article or reference]. The necessary level of expert knowledge shall be determined in particular according by the data processing carried out and the protection required for the personal data processed by the controller or the processor.

The controller or the processor ensures that any other professional duties of the data protection officer are compatible with that person's tasks and duties as data protection officer and do not result in a conflict of interests.

The data protection officer shall be appointed for a period of at least four years. The data protection officer may be reappointed for further terms. During the term of office, the data protection officer may only be dismissed from that function, if he or she no longer fulfils the conditions required for the performance of his or her duties.

Concern 23 OCL rule **NONE**

Concern 24 name **Article 25**

Concern 24 add. Fields **Accountability: cooperation with supervisory authority** sharing, access to system

Concern 24 contents

The controller and the processor shall cooperate, on request, with the supervisory authority in the performance of its duties, in particular:

- by providing access to all personal data and to all information necessary for the performance of its supervisory duties,
- and by granting access to any of its premises, including to any data processing equipment and means, in accordance with national law, where there are reasonable grounds for presuming that an activity in violation of the provisions adopted pursuant

to this Directive is being carried out there, without prejudice to a judicial authorisation of required by national law.

The controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

Concern 24 OCL rule **NONE**

Concern 25 name **Article 19.1**

Concern 25 add. Fields **Data Protection by design**

Concern 25 contents

Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor if any shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject, in particular with regard to the principles laid out in Article 4. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment, the results shall be taken into account when developing those measures and procedures.

Concern 25 OCL rule **NONE**

Concern 26 name **Article 21**

Concern 26 add. Fields **Subcontracting (processor)**

Concern 26 contents

Where a processing operation is carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organisational measures governing the processing to be carried out and to ensure compliance with those measures.

The carrying out of processing by means of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall

- (a) act only on instructions from the controller;

- (b) Employ only staffs who has agreed to be bound by an obligation of confidentiality or are under a statutory obligation of confidentiality;
 - (c) Take all required measures pursuant to Article 27 [link to article or SALT reference];
 - (d) Engage another processor only with the permission of the controller and therefore inform the controller of the intention to engage another processor in such a timely fashion that the controller has the possibility to object;
 - (e) insofar as it is possible given the nature of the processing, adopt in agreement with controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III [link to article or SALT reference];
 - (f) Assist the controller in ensuring compliance with the obligations pursuant to Articles 25a to 29 [link to article or SALT reference];
 - (g) Return all results to the controller after the end of the processing and not otherwise process the personal data and delete existing copies unless Union or Member State law requires its storage;
 - (h) Make available to the controller and the supervisory authority all the information necessary to verify compliance with the obligations laid down in this Article;
 - (i) Take into account the principle of data protection by design and default
- The controller and the processor shall document in writing the controller's instructions and the processor's obligations.

Concern 26 OCL rule **NONE**

Concern 27 name	Article 19.2
Concern 27 add. Fields	Data Protection by default
Concern 27 contents	

The controller shall ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data. (Art.19.2)

Concern 27 OCL rule **NONE**

Concern 28 name	Article 27
Concern 28 add. Fields	Security
Concern 28 contents	

The controller and the processor should implement appropriate technical and organisational measures and procedures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation

In respect of automated data processing, the controller or processor, following an evaluation of the risks, should implement measures designed to:

- (a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);
- (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
- (c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
- (d) prevent the use of automated data processing systems by unauthorised persons using data communication equipment (user control);
- (e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control)
- (f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);
- (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the data were input (input control)
- (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);
- (i) ensure that installed systems may, in case of interruption, be restored (recovery);
- (j) (j) ensure that the functions of the system perform, that the appearance of faults in
- (k) the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity);
- (l) (ja) ensure that in case of sensitive
- (m) personal data processing according to Article 8, additional security measures have to be in place, in order to guarantee situation awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data

Processors may be appointed only if they guarantee that they observe the requisite technical and organisational measures.

Concern 28 OCL rule **NONE**

end

3.2.8 General Data Protection Regulation

System type	All
Reference name	EU data Protection Regulation Proposal (not approved yet)
Context:	EU
Context: free fields	All processing of personal data except certain specific processing
Concern 1 name	Article 23
Concern 1 add. Fields	Accountability: general obligations

Concern 1 contents

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 (IP) is required to document and communicate in an appropriate way all privacy related policies, procedures and practices.

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 organisational 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.

Concern 1 OCL rule NONE

Concern 2 name	Article 32a
Concern 2 add. Fields	Data Protection Impact Assessment

Concern 2 contents

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. 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 Article 44(1), the documentation of appropriate safeguards;

Accountability requirements

Policies: 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: 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: 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.

Concern 2 OCL rule NONE

Concern 3 name Article 32a

Concern 3 add. Fields Data Protection Impact Assessment, periodic reviews

Concern 3 contents

Periodic reviews should also include reviews of PIA, privacy policies and purposes of the system. The review should be documented and could be used to prove that the data controller is compliant with data minimisation principle and that data are collected for defined purposes. For example, if a video surveillance system has been set up for prevention and deterrence purposes, these purposes may change under certain situations.

Concern 3 OCL rule NONE

end

3.3 Socio-ethical artifacts

3.3.1 Introduction to Socio-Ethical artifacts

As for legal artifacts, the goal of this document is to show typical references of Socio-Ethical type that could be selected upon the elaboration of a SALT instance dedicated to the WP5 use

cases. Especially in the moving field of public perception, societal balance about privacy risks and surveillance benefits towards individual security, the exhaustiveness is not at stake.

The SALT framework that will be used during the WP5 demonstrations and test will embed the artifacts presented below. It may also contain some more references, enabling to depict completely the manual choice process that is performed while building the applicable SALT instance.

3.3.2 Table of proposed Socio-Ethical artifacts in this document

As for the legal references, this section embeds a summary table of the Socio-Ethical references that are detailed below. The nature of the video-surveillance system considered in the WP5 use cases (use of video records for investigations from cameras placed in public space, from 2 different points of view: privacy protection in the first use case, and accountability of operators in the second one) does not let many degrees of freedom regarding the deployment of the use case itself, as its main surveillance capabilities and goals are embedded in its description.

The concerns here presented in the form of SALT references might be of interest mainly when discussing and deciding the green-field deployment of video-surveillance system by public authorities: the system would in this case not be in place and the pieces of information stored in the Framework would be used to assess the need for this system (including performing the “balance” or the “win-win choices” among performance from the surveillance point of view, and the privacy harms from another point of view).

The fact that this content might not be fully applicable to the use case is not a problem, as the normal use of the Framework consists of a selection by the stakeholders of the applicable references.

The table below sums up the Socio-Ethical references documented further in the document and their applicability to the WP5 use cases, using the following annotation:

- May be applicable to use-case 1 (privacy preserving law enforcement to video archive search)
- May be applicable to use case 2 (accountability of video-surveillance operators)
- Rather provided as SALT example contents.

This is depicted in the table as specified below:

- *** reference highly likely to be selected within the use case context,
- ** reference likely to be selected within the use case context,
- * reference less likely to be selected within the use-case context

References description. Fields	References descriptions	Applicability to use-case 1	Applicability to use-case 2	Example
Reference name	2008 CNIL study : French people and videosurveillance”	*	*	***
System type	All video-surveillance systems			
Context	Worldwide			
Reference name	“Surveillance ethics from the Internet Encyclopedia of Philosophy”			***
System type	All surveillance systems			
Context	Worldwide			
Reference name	“video-surveillance in retail places: ethical perspective ”			***
System type	All surveillance systems			
Context	Worldwide			

Table 2: list and applicability of SALT Socio-Ethical references to the WP5 Use-Cases

3.3.3 2008 CNIL study: “French people and videosurveillance”

This reference is raised by a study conducted in 2008 in France for the CNIL (the French DPA). It is here considered that this study might be of interest for systems deployed all over the world, but keeping in mind that it has been realized in France.

System type	Video-surveillance systems
Reference name	2008 French survey on video-surveillance
Context:	Worldwide
Context: free fields	NA
Concern 1 name	perception of efficiency of cameras
Concern 1 add. Fields intention	Socio-Ethical, individual participation, consent and choice,

Concern 1 contents

Statistical answer to the question: “do you think that dramatically increasing the number of video-surveillance cameras in public space enables efficient combat against crime and terrorism?”

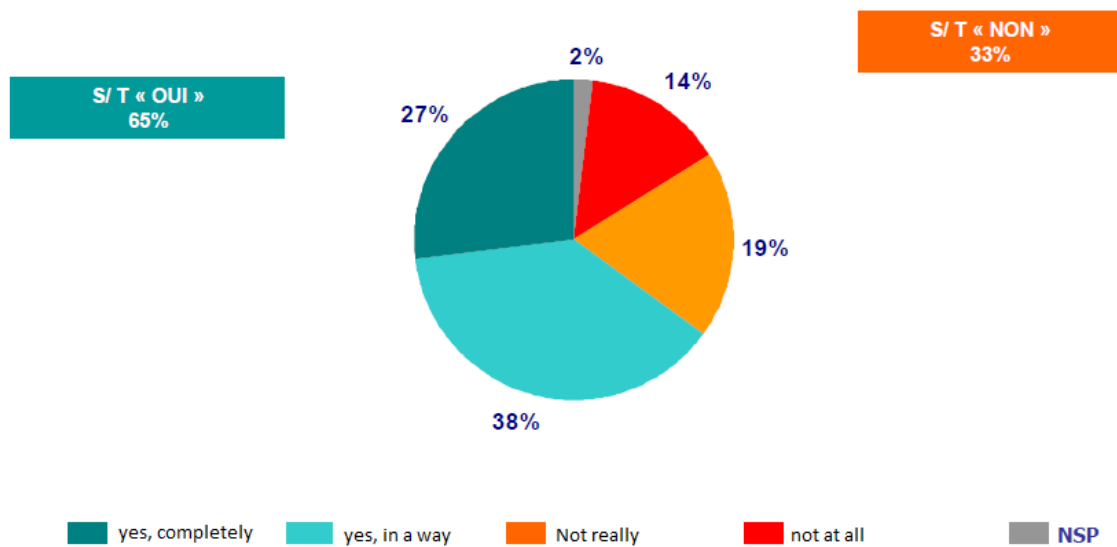


Figure 11: perception of video-surveillance cameras by the French population (from [2])

Concern 1 OCL rule NONE

Concern 2 name	importance of controls on video-surveillance cameras placed in public space
Concern 2 add. Fields intention	Socio-Ethical, individual participation, consent and choice,

Concern 2 contents

Statistical answer to the question: “do you think it is very important, important, not really important, not at all important that an independent body controls these video-surveillance systems to guarantee adequate respect of privacy policy”?

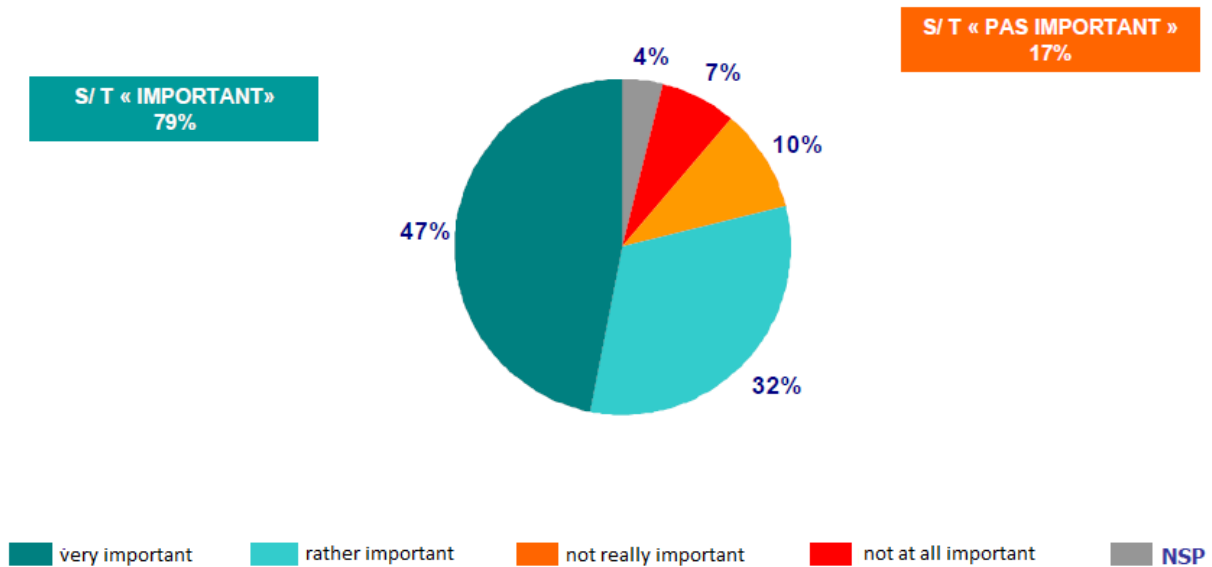


Figure 12: perception of the importance of the surveillance in public space by French population (from [2])

Concern 2 OCL rule NONE

Concern 3 name general opinions about video-surveillance

Concern 3 add. Fields Socio-Ethical, individual participation, consent and choice, intention

Concern 3 contents

Statistical answer to the question: “generally speaking, do you strongly agree, rather agree, rather disagree, strongly disagree about presence of video-surveillance cameras in public space?”

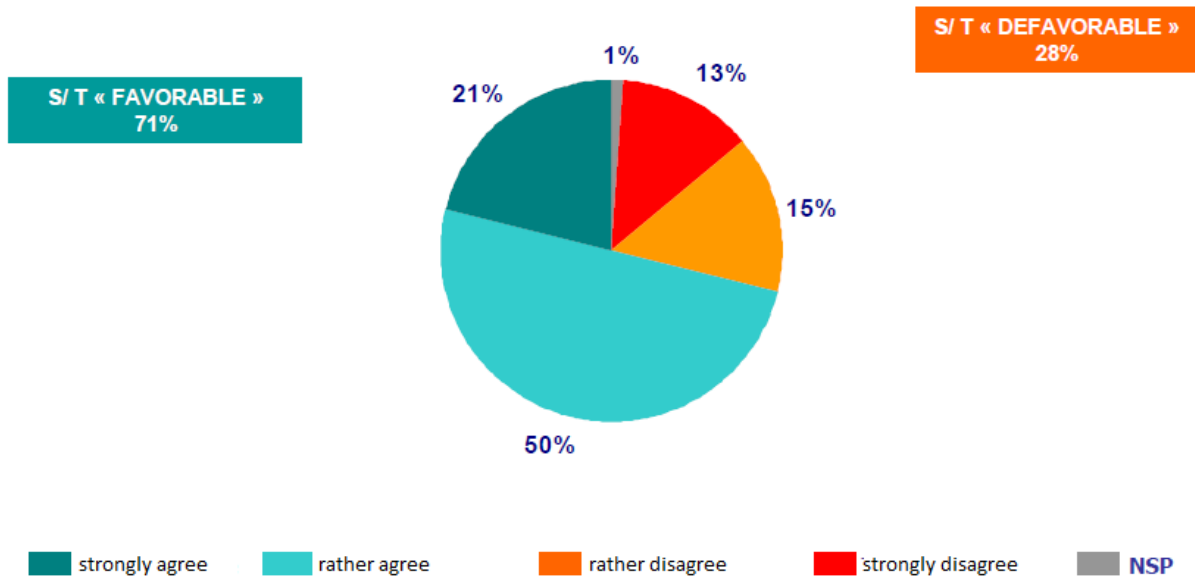


Figure 13: general agreement about the installation of video-surveillance cameras in the French population (from [2])

Concern 3 OCL rule NONE

end

3.3.4 “surveillance ethics” from Internet Encyclopedia of Philosophy (IEP)

This reference is entirely extracted from the webpage <http://www.iep.utm.edu/surv-eth/>, an article from Kevin MACNISH, from the University of Leeds, United Kingdom.

System type	All systems
Reference name	Ethics of surveillance from a philosophical perspective
Context:	Worldwide
Context: free fields	NA
Concern 1 name	full article
Concern 1 add. Fields	Socio-Ethical, individual participation, consent and choice, intention

Concern 1 contents

Surveillance Ethics

Surveillance involves paying close and sustained attention to another person. It is distinct from casual yet focused people-watching, such as might occur at a pavement cafe, to the extent that it is sustained over time. Furthermore the design is not to pay attention to just anyone, but to pay attention to some entity (a person or group) in particular and for a particular reason. Nor does surveillance have to involve watching. It may also involve listening, as when a telephone conversation is bugged, or even smelling, as in the case of dogs trained to discover drugs, or hardware which is able to discover explosives at a distance.

The ethics of surveillance considers the moral aspects of how surveillance is employed. Is it a value-neutral activity which may be used for good or ill, or is it always problematic and if so why? What are the benefits and harms of surveillance? Who is entitled to carry out surveillance, when and under what circumstances? Are there any circumstances under which someone should never be under surveillance?

This article provides a brief overview of the history of surveillance ethics, beginning with Jeremy Bentham and George Orwell. It then looks at the development of surveillance studies in the light of Michel Foucault and the challenges posed by new techniques of surveillance which allow unprecedented collection and retention of information. The bulk of this article focuses on considering the ethical challenges posed by surveillance. These include why surveillance is undertaken and by whom, as well as when and how it may be employed. This is followed by an examination of a number of concerns regarding the impact of surveillance such as social sorting, distance and chilling effects.

Table of Contents

Origins

Recent History

Privacy

Trust and Autonomy

Cause
Authority
Necessity
Means
Social Sorting
Function Creep
Distance
Chilling Effects
Power
References and Further Reading

1. Origins

Jeremy Bentham's idea of the Panopticon is arguably the first significant reference to surveillance ethics in the modern period (Bentham 1995). The Panopticon was to be a prison, comprising a circular building with the cells adjacent to the outside walls. In the center was a tower in which the prison supervisor would live and monitor the inmates. Large external windows and smaller internal windows in each cell would allow the supervisor to monitor the activities of the inmates, while a system of louvres in the central tower would prevent the inmates from seeing the supervisor. A rudimentary form of directed loudspeaker would enable the supervisor to communicate with the prisoners. Through not knowing when they were under surveillance, Bentham argued, the inmates would come to assume that they were always under surveillance. This would encourage them to be self-disciplined and well-behaved during their incarceration. The prospect of living in this way would also deter those who visited the prison from wanting to commit crimes. Hence the Panopticon would serve as a deterrent to the inmates from misbehaving or committing future crimes and to general society from committing crimes and finding themselves so incarcerated.

George Orwell's 1984 extended the Panopticon to encompass the whole of society, or at least the middle classes (Orwell 2004). In this novel the Panopticon became electrical with the invention of the telescreen, a two-way television which allowed the state almost total visual and auditory access to the homes, streets and workplaces of the citizens. As the inmates of the Panopticon were reminded of the supervisor's presence by the loudspeaker, so citizens in Orwell's vision were told repeatedly that "Big Brother is watching you". Orwell used the novel to discuss, among other things, both the reasons of the state for wanting ubiquitous surveillance and the impact that this has on the individual and the nature of a society under ubiquitous surveillance.

*The theme of the Panopticon was revisited by Michel Foucault in *Discipline and Punish*, an overview of the history of prisons and the value they serve (Foucault 1991). Foucault's particular concern was with the use of power and its increasing bureaucratization in the modern period. His study began with torture and the emphasis on the sovereignty and power of the king. With the Enlightenment the prison was introduced as a more efficient means of punishment, supported by society's increasing acceptance of the value of discipline beyond merely the military or religious arenas. Oversight became a fundamental tool in enforcing discipline, and so the Panopticon served as both a means of punishment and a form of discipline of the inmates,*

owing to the seemingly persistent gaze of the supervisor. With time, Foucault argued, the prison was combined with the workhouse and the hospital to simultaneously deprive inmates of their freedom whilst attempting to discipline and reform them.

Aside from Foucault's comments on the nature of prisons and their value in society, his reference to the Panopticon introduced the concept to a new generation of scholars unfamiliar with Bentham's penal theories. As such it is the Panopticon read through the lens of Foucault, along with Orwell's dystopian vision, that came to dominate early discussions of surveillance and its impact on society and the individual.

2. Recent History

While Bentham/Foucault and Orwell successfully raised questions about the value and harms of surveillance, these had limited impact in many philosophy departments [...]

[...]

Concern 1 OCL rule **NONE**

end

3.3.5 “video surveillance research in retailing: ethical issues”

This reference contents is purchasable from the webpage <http://www.emeraldinsight.com/doi/abs/10.1108/09590550010356831> , an article from Kevin MACNISH, from the University of Leeds, United Kingdom.

System type	video-surveillance in retail places
Reference name	“video-surveillance research in retailing: ethical issues”
Context:	Worldwide
Context: free fields	retailing, consumer behavior
Concern 1 name	full article
Concern 1 add. Fields	Socio-Ethical, individual participation, consent and choice, use, retention and disclosure, intention

Concern 1 contents

Abstract:

In an increasingly competitive market there is a keen interest among retailers to understand as much as possible about consumer behavior. Advances in technology have presented retail marketers with many new research tools with which to monitor such behavior. Alongside such advances in technology, however, have come accusations that some aspects of marketing and marketing research raise ethical issues. Those engaged in the use of new marketing and research methods therefore need to be aware of any potential public concerns and be seen to adhere rigorously to ethical practice. This paper examines the growing use of video surveillance within retail stores. The technique offers an objective and accurate research tool for retailers to monitor consumer behavior. However, along with increasing use comes the potential danger of

abuse and the paper finds that few guidelines exist to assist retailers or researchers in managing this type of research.

Concern 1 OCL rule **NONE**

end

3.4 Technical artifacts

3.4.1 Introduction to technical artifacts

This part of the document is dedicated to provide examples of SALT technical artifacts, especially providing usable technical guidance for the 2 WP5 use cases, dedicated to the use by public forces of video-surveillance data for investigation purposes. Other artifacts, maybe of lower interest for the WP5 use cases, may be integrated in order to fully illustrate the type of information that can be handled by the SALT framework.

The technical artifacts are the ones that are most often the closest to the design phase, implying technical stakeholders such as engineers, designers of surveillance systems. Nevertheless, the selection of the references to build a SALT instance for a given context of interest is intended to be realized collectively, implying non-technical experts (maybe sometimes even without technical experts). The technical artifacts are for this reason to be readable at least regarding their field of application and main principles and guidelines by any stakeholder likely to use the SALT framework.

When prescription and verification rules about the system are embedded, these rules are expressed using the OCL form, which makes them applicable to engineering designs of the surveillance systems proposed in the SALT Framework, expressed within UML diagrams. Each concern of a reference is likely to embed one or several OCL rules. When the selection of a reference is performed, the person or the team performing this selection has the possibility to discard or to apply the rule (the choices performed being traced in the SALT reference in order that the choices performed are accountable).

In this document, the OCL rules are expressed in natural language. The goal here is to explain the type of requirement they embed rather than being formally exact. The integration of these rules in strict OCL compliant shape is to be performed as future actions in the scope of the project, especially within WP3 and WP4 work-packages.

Even regarding technical artifacts, the selection process is non-deterministic, meaning that for one given surveillance context there is not a unique answer provided by the SALT framework (a unique selection of SALT references), but a result of an informed and accountable choice performed by a person or a team.

3.4.2 Table of proposed technical artifacts in this document

The technical artifacts presented here are to be considered as an example set of artifacts. As exhaustiveness is not the goal (nor even possible, the knowledge to embed being huge), some more may be added in the SALT framework after the release of this document.

The main topics that are considered in SALT technical artifacts are description of technical devices, systems and of their surveillance performance, the description of privacy harms linked to these devices and systems, and the description of Privacy Enhancing Technologies

The table below sums up the technical references documented further in the document and their applicability to the WP5 use cases, using the following annotation:

- May be applicable to use-case 1 (privacy preserving law enforcement to video archive search)
- May be applicable to use case 2 (accountability of video-surveillance operators)
- Rather provided as SALT example contents,
- Describes technical devices and systems,
- Embeds privacy enhancing technologies,
- Embeds privacy harms description

This is depicted in the table as specified below:

- *** reference highly likely to be selected within the use case context,
- ** reference likely to be selected within the use case context,
- * reference less likely to be selected within the use-case context

References description. Fields	References descriptions	Applicability to use-case 1	Applicability to use-case 2	Example	Technical descriptions	Privacy risks	PET
Reference name	CNIL Security Guide	**	**	***	*	**	**
System type	All						
Context	France						
Reference name	Denial of service risk IT attack on camera	**	**	***	**	***	***
System type	All video-surveillance systems						
Context	Worldwide						

Reference name	Encryption of video data: principles and benefits						
System type	All video-surveillance systems	**	*	***	**	*	***
Context	Worldwide						
Reference name	Logical access control to video-surveillance systems						
System type	All video-surveillance systems	***	**	***	*	**	***
Context	Worldwide						
Reference name	Capabilities of google-glass cameras						
System type	All video-surveillance systems			***	**	*	*
Context	Worldwide						
Reference name	Logs and audit tools about operator actions for enhanced accountability						
System type	All surveillance systems	*	***	***	**	*	***
Context	Worldwide						
Reference name	Data lifecycle Management: monitoring and erasing tools						
System type	All video-surveillance systems		***	***	**	*	***
Context	Worldwide						
Reference name	Resolution of video images and recognition performances						
System type	All video-surveillance systems	*		***	***	***	***
Context	worldwide						

Table 3: contents of technical references and their applicability to WP5 use cases

3.4.3 France - Security Guide (CNIL)

System type	All
Reference name	CNIL Security Guide
Context:	France
Context: free fields	NA
Concern 1 name	Security: authorisation management
Concern 1 add. Fields	data integrity, data quality, confidentiality
Concern 1 contents	

Securing an IT system requires taking into account all aspects of its management. This security resorts to the respect of good practices and the maintenance of the data-processing tool in a state-of-the-art condition with regard to the attacks to which it can be subjected. However, this security will only be effective if rigor is applied to the delivery (and the withdrawal) of security clearances as well as the processing of some unavoidable incidents. In order to guarantee that all IT system users only have access to the data they need to know, two elements are necessary:

- providing a unique identifier to each user, in association with authentication means: an authentication method;
- applying prior access controls to data for each category of users: an authorisation management.

Concern 2 name	Security: keeping records and documentation of data processing operations
Concern 2 add. Fields	data integrity, data quality, confidentiality

Concern 2 contents

The Privacy Management Program/internal privacy policy should indicate practices and policies which would allow keeping records and documentation of operations performed upon personal data. Operations performed upon personal data may include but not limited to data collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (Art. 17 Directive 95/46/EC). Maintaining documentation would allow to prove that the controller has collected and processed personal data in a fair and lawful manner (Article 6 al. French DPA Act) for determined, explicit and legitimate purposes (Article 6 al.2 French DPA Act).

These requirements can only be assessed by observing how the IT system is used. Consequently, it is necessary to implement a logging facility, i.e. recording each user's actions on the system during a defined period of time.

Concern 3 name	Security: storage
Concern 3 add. Fields	data integrity, data quality, confidentiality

Concern 3 contents

The Privacy Management Program/internal privacy policy should indicate practices and policies which would allow ensuring the secure storage of collected personal data.

In the video surveillance and video archive search system the recorded videos are stored in the NVR (Network Video Recorder). Namely, NVR is used to store video input from cameras over networks, and enable remote access to video data from the cameras.

To protect against leakage of personal data, the video footages should be stored in an encrypted form in the video databases.

The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. Except for law enforcement bodies, images will not be provided to third parties. Ensuring security of the obtained data could provide assurances that data is not use for further processing.

Concern 4 name	Security: incident management
-----------------------	--------------------------------------

Concern 4 add. Fields	Accountability, Data integrity, data quality, confidentiality, data minimization
------------------------------	---

Concern 4 contents

The Privacy Management Program/internal privacy policy should indicate practices and policies which would allow to provide an effective and timely response in case of an incident. Any data processing entails risks and therefore, the controller should develop practices and policies to handle incidents prior to launching a surveillance system.

3.4.4 Denial of Service risk and possible remediation

This reference is dedicated to a specific harm and to its remediation: the risk that an unprotected camera is put out of service by an IT attack using the Denial of Service method.

System type	Video-surveillance systems
Reference name	Denial of service IT attack on a camera: risks and possible remediation
Context:	Worldwide
Context: free fields	hacker, IT attack
Concern 1 name	description of risk
Concern 1 add. Fields	technical, data collection

Concern 1 contents

Many commercially available devices (video cameras) can be stopped from standard operation using an IT attack. The main condition for this to occur is that it is possible to physically connect to the IT network on which the camera is connected.

Description of the attack:

An important number of fake connections are launched on the device (especially on the management port). Even if the camera is protected by authentication means, many camera models will enter a protection mode by stopping the operation. Then the data collection stops and the performance of the system is decreased (possibility of crimes without recording of the footages).

Concern 1 OCL rule	NONE
---------------------------	-------------

Concern 2 name	possible remediation to DoS attack on a camera: temporization
Concern 2 add. Fields	technical, data collection, conception, development, verification

Concern 2 contents

A temporization between the submission of a request to the camera on the management port and the answer to the request is implemented.

Concern 2 OCL rule	camera: delay of answers on management port activated
---------------------------	--

Concern 3 name possible remediation to DoS attack on a camera: network hardening using 802.1X network-level authentication

Concern 3 add. Fields technical, data collection, conception, development, verification

Concern 3 contents

The network is equipped with devices (switches, cameras) capable of performing 802.1X authentication. This allows preventing from the connection of any unexpected or unauthorized additional connection on the network likely to perform the DoS attack.

Concern 3 OCL rule 1 802.1X authentication activated on the cameras

Concern 3 OCL rule 2 802.1X authentication activated on the network devices

end

3.4.5 Encryption of video data

System type video-surveillance systems

Reference name Encryption of video data: principles, technologies and benefits

Context: Worldwide

Context: free fields SSL, HTTPS, encryption

Concern 1 name main principles and benefits of video data encryption

Concern 1 add. Fields technical, conception, development, verification, collection limitation, use, retention and disclosure limitation, information security

Concern 1 contents

The encryption of the video streams, even if not simple to perform, brings many gains: it allows preventing the unexpected, unauthorized viewing of the video-stream issued from the video-surveillance camera to happen.

The encryption of streams is mainly applicable to IP (network) cameras, rather than analogical cameras. Nevertheless, the wide systems, with many cameras and long-path cables are for most of them based on IP technology.

The main gains of the encryption of the streams are linked to the prevention of unexpected disclosure of these streams: this provides enhanced privacy level of the person within the field of view of the cameras, but also greater security when the topics being filmed are critical (sensible information, critical sites).

The drawbacks of the encryption is the cost of the IT infrastructure to deploy, which is often far more important than a simpler one without encryption capability. Moreover, it can be seen sometimes as a drawback that it might be more difficult to access to streams of interest when the need is urgent (e.g. somebody needing the unexpected access to a stream from a protected

Concern 1 add. Fields **Technical, conception, development, use, use, retention and disclosure limitation, accountability**

Concern 1 contents

Role Based Access Control

The Right to manage data (watch a real-time or recorded stream) is controlled thanks to a role attribute granted to each of the users of the system. Every user is assigned to one or several groups or roles and has rights of these groups, defined for each one from its mission needs.

Concern 1 OCL rules: the access to the images is protected by an Role-Based Access-Control mechanism

end

Concern 2 name **Attribute-based access control**

Concern 2 add. Fields **Technical, conception, development, use, use retention and disclosure limitation, accountability**

Attribute Based Access Control

The ABAC access control method to the cameras streams is based on policies that can vary over time, position, etc. The implementation can be based on XACML (eXtensible Access Control Markup Language).

Every permission record - policy entry - has several attributes:

- users (subject)
- validity (environment)
- permissions (groups of attributes)
 - cameras & their time frame (resource)
 - algorithms (action)

A notable difference between traditional access control systems and ABAC is that a request does not contain the action or resource. The user is authorized by subject and environment (time) only. Instead of requesting a specific resource, the user is presented all resources he is allowed to access, grouped by policy.

Concern 2 OCL rules: the access to the images is protected by an Attribute-based Access Control mechanism

end

3.4.7 Capabilities of Google Glass cameras

This reference is an example of technical prospective reference where information is given about new technical possibilities and new fields of application of technical devices. This type of reference won't give rise to OCL rules.

System type	video surveillance systems
Reference name	technical capabilities of "Google glass" cameras
Context:	Worldwide
Context: free fields	wearable devices, innovation in video surveillance
Concern 1 name	description of Google glass and their use
Concern 1 add. Fields	Technical, Socio-Ethical, data collection, use, retention and disclosure limitation, privacy compliance
Concern 1 contents	

The Google glasses are glasses equipped with miniaturized devices that enable their wearer:

- To see video information in his field of vision (including augmented reality, meaning information contextualized from information such as position, ongoing task...)
- Thanks to an embedded camera and micro, to film and to send video and audio streams to external devices using a WIFI connection



Figure 14: photography of Google glasses (from en.wikipedia.org)

Concern 1 OCL rule **NONE**

Concern 2 name	possible privacy harms and remediation
Concern 2 add. Fields	Technical, Socio-Ethical, data collection, use, retention and disclosure limitation, privacy compliance, conception, development, specification

Concern 2 contents

The Google glass devices enables privacy harms by allowing very discrete video capture, sending, and recording.

Within some public places, the choice has been made to forbid the use of Google glasses. A solution to limit the risk of privacy harming would be to prevent the data transmission to occur, e.g. by jamming the WIFI Radio-Frequency band.

Concern 2 OCL rule **the system contains a jammer active in WIFI band**

end

3.4.8 Operators actions logging

System type	video-surveillance systems
Reference name	Logs and audit tools about operator actions for enhanced accountability
Context:	Worldwide
Context: free fields	auditability, operator's actions, logging
Concern 1 name	benefits and methods for operators' actions logging
Concern 1 add. Fields	technical, conception, development, use, accountability

Concern 1 contents

The video-surveillance system is used by operators. These operators have to enter the system by login (most often using a personal account on the system). Then they perform their tasks using the controls provided by the software they use. These controls are mainly commands about the cameras and recorded video-streams connected to the system and that they are authorized to use. These controls are for the most basic ones display commands, cameras zooming and movement commands, image capture commands.

Recording the actions of the operators (at least some of the actions) enables to trace who performed what on the system, but also who viewed what (or at least who had the possibility to view what). Basically, a recording (or tracing) system is logging text traces the actions of the operators commands, with their identifiers, enabling to go back to the identity of the author of any action.

An auditing tool is often used to help post-analysis and research about what happened during a particular circumstance or event. The privacy of the operator himself nor his rights granted by labor and employment law shall not be infringed.

Concern 1 OCL rules: the action of the operators shall be recorded by and auditing tool

end

3.4.9 Resolution of video images and recognition performances

System type	video-surveillance systems
Reference name	Resolution of video images and recognition performances
Context:	Worldwide
Context: free fields	resolution, balance between security and privacy
Concern 1 name	recognition performance versus image resolution
Concern 1 add. Fields accuracy and quality	Technical, conception, development, collection limitation,
Concern 1 contents	

The resolution of an image is a very important parameter to assess its quality (even not the only one, the distortion due to optical parameters, or dynamic, capability to image very different level of light in the same scene are also important contributors to the image quality).

The raw resolution of an image is important (e.g. HD 720p, 4K), but even more is the resolution within the physical world. It is expressed in PPF (Pixel per Foot), and quantifies the number of unitary pieces of information that are recorded on the object or person viewed.

An illustration of the strength of the resolution upon image embedded information is shown below (image from a Whitepaper from the MOTOROLA firm⁷).

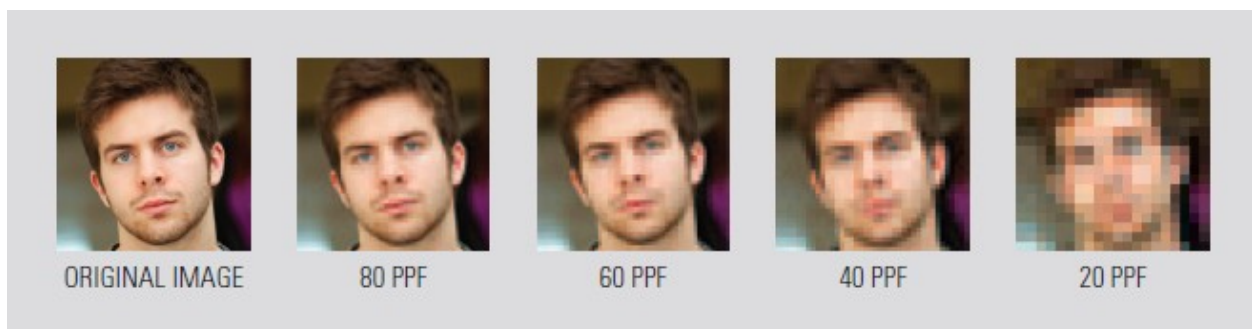


Figure 15: impact of image resolution upon the potential performance of a video-surveillance system

It is generally recognized that 40PPF is the needed resolution for possible face identification, while 80PPF is needed for license plate reading.

This physical resolution appears very important to assess during the conception of a video-surveillance system. It can be seen as a prominent feature for balancing the privacy and the security provided by the system: The higher the physical resolution is the higher the recognition

7

http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.motorolasolutions.com%2Fweb%2Fbusiness%2FDocuments%2Fstatic%2520files%2FVideoSurveillance_WP_3_keywords.pdf&ei=P8OJVOG4AsvsUsmQg4qP&usq=AFQjCNEOIRpGeJH-A44jZ-CM4sYNHUTDcw&sig2=x-BH98qTGti6ZmKVE_aE6A&bvm=bv.81456516,d.d24

performance is. So the higher the physical resolution is, the higher the security level is, the lower the privacy is.

The physical resolution remains nevertheless difficult to assess, because it varies with the distance of the observed object or person, and with the zooming level of the cameras. Nevertheless simulators enable to predict this physical resolution criterion.

OCL rules

end

4 Specification of VAS use-case 1 and risks related to privacy and accountability

The VAS Use Case 1 specification is refined in this document. Coherently, a list of test cases of the design of the system is proposed in the form of misuse cases. These misuse cases, if allowed by the system, would lead to actual consequences on the privacy of one or several stakeholders of the system.

Some of these misuse cases will be used within the project to test the impact of use the SALT framework against these cases. In other words, it will be demonstrated that a correct use of the SALT framework (provided it is populated with adequate contents) enables to raise (at build stage or use stage) measures that prevent misuse cases to occur and harm privacy.

4.1 Specification of VAS use case 1: privacy-preserving law enforcement access to video archive search

Short Description:

Law enforcement agency (LEA) searches video surveillance archives at Infrastructure Provider (IP) in crime investigation.

Main actors:

- LEA
- PO
- Controller
- DPO
- DPA
- Victim
- TP

Use case aim:

To allow PO secure remote access to video archive data at IP, privacy-preserving video archive search for analyse and collect evidence for crime investigation

Preconditions:

- Legal recording permission for IP
- Accepted viewpoint for involved cameras by DPA
- A crime has been committed

Scenario description:

A crime is committed in the premises of an IP (e.g. railway operator). The crime does not interfere with the security rules of the IP (not significant for safe operation of their systems) because it is not the responsibility of the IP. For this use-case it is sufficient to assume that it is

a typical crime (theft or assault) and it is within the responsibility of the law enforcement agencies.

The victim reports the crime to the police. At this moment personal data is involved in the use-case. Information on time, place, actors and description is assembled into a “case”. The “case” is entered by the PO in paper or electronic form according to some predefined workflow of the LEA. Depending on the LEA’ resources or the urgency of the crime, it sooner or later enters the stage of “collecting evidence”. Implicit knowledge reveals that the crime might have been recorded by the video surveillance system operated by the IP. For simplicity, it is assumed that the PO in charge of the case crime is the same person investigating the video data.

The PO asks the IP for the video footage to look for evidence that something had happened and to secure the evidence. Therefore the PO has to be recognized as a legally authorized person to access and view the video data. This authorization should be formally proved and recorded. This might involve Judge and DPA. If this has happened, the IP, represented by the DPO for this specific case is allowed to hand over video data. The amount of data is restricted to the necessary data for this case. Permission for the PO should be restricted to the amount of cameras involved, to the time of the crime.

The PO needs to query the video archive and retrieve video data. At this point the real police forensic work starts. The PO investigates the scenes and tries to gather evidence. Any data access more than permitted is blocked. Typically it takes time to find the relevant scenes in the video footage. Often more data captured by different cameras are needed to facilitate the investigation (e.g. to find the suspect, accomplices or hints for a better pursuit of the offenders or to retrieve a better frontal face snapshot during entry to the train station). This work is entitled “video forensic search”.

As mentioned, it could be possible that during this forensic search an extended permission, it is needed to access more data. This process should be formally proved and logged as well.

If evidence is gathered, relevant video footage should be secured and provided in a form that can be transferred and presented at the court as evidence. The rest of the retrieved data must be deleted according to the specification of the data life cycle management.

To fulfil this task, after the approval from the Judge, the LEA contacts the TP and IP to design and develop a video archive search system, which will allow a PO to remotely access and search the video data at the IP within the LEA premise during an on-going investigation. The TP is contracted for design and development of the technical solution. To address the challenge of privacy concerns, the TP leverages the SALT framework and involves SE. In addition, the DPA is involved to provide the oversight of all privacy-related issues.

Video archive search user story

The user story is taken from a PO’s view. For the global system architecture see Section 2.2.

1. The PO asks the DPO to open a new case / creates a digital permission for a specific search.

2. Privacy Enhanced Access Control (PEAC) [peek] provides an interface for communication with the VAS and an administrative interface for editing permissions with their permissions. Administrators can log into PEAC using the web interface. There they are able to create, edit and delete Permissions, Cameras, Algorithms, Infrastructure Providers (NVRs) and Users. Users themselves are not managed by PEAC. It only creates local database entries for needed users for easier data management. PEAC uses the WSO2 Identity Server as abstraction layer for user authentication. The Identity Server provides a unified interface for PEAC and can be connected to LDAP or Active Directory, but can also be used with Federal Authentication Systems such as OpenID, OAuth, SAML or Passive STS. PEAC also fetches available cameras from the configured NVRs and populates the database as to make management easier for the Administrator.

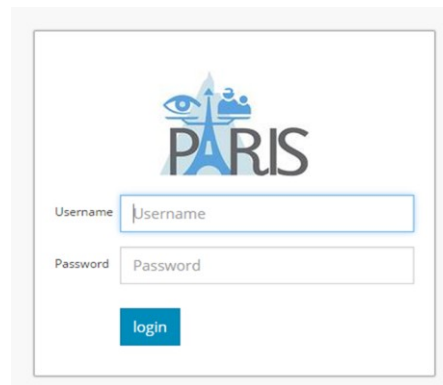
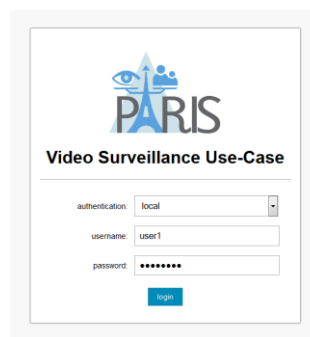


Figure 16: authentication panel to PEAC, Privacy Enhanced Access Control

3. A PO can login at the VAS client by typing in username and password.



4. The VAS client will authenticate the user against the PEAC server.
5. If the authentication of the user has been approved by the PEAC server, the list of all cases associated to the user is send to the VAS client. So the user will only be able to access video source and perform actions according to predefined permissions created by the DPO according to the privacy policy.

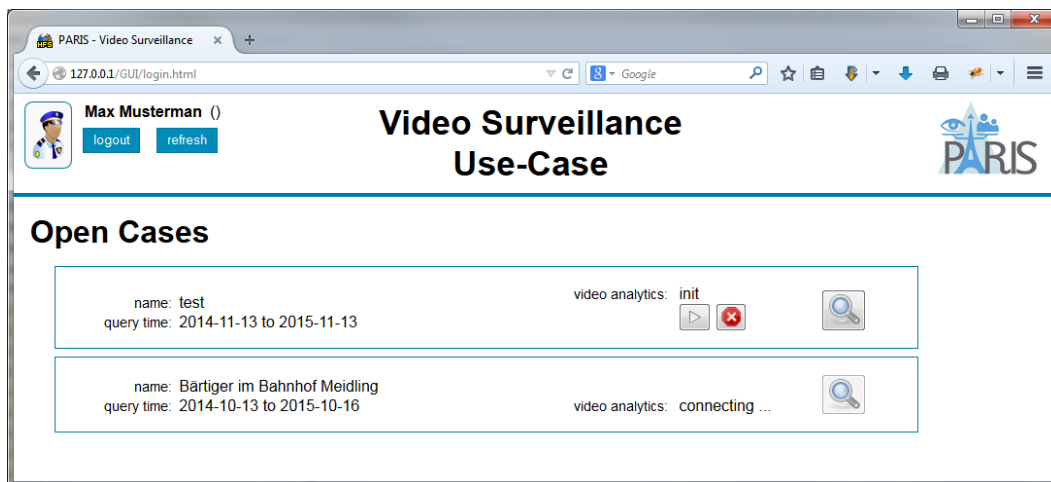


Figure 17: access to video-surveillance cases panel

6. The user can perform various search actions depending on the state of each case.
 - a. If a search has been created and initialized, the PO can start the search. The actual search will be done as an independent background task and the user will be notified as soon as the processing has finished.
 - b. Intermediate results of currently processed searches can be viewed. So the PO does not have to wait until the whole video has been analysed to get the first results.
 - c. Results of completed searches can be accessed immediately, as long as the digital permission is still valid.
 - d. All search requests can be stopped and reset if necessary.

7. The algorithm used in this use case demonstrator scans the videos for all persons appearing in a given timespan. A list of thumbnail images of detected persons will be displayed. A given person can be linked to the video and time where and when it appears in. This information can be used to access the associated surveillance video



Figure 18: automatic persons detection and extraction principle

8. All accesses and search requests by the VAS are based on the permissions granted by the PEAC which is enforcing the privacy and access control policies. Illegitimate requests (e.g. additional search algorithms or to not approved videos / timespans) are excluded

by design. The user has access to the approved permissions only and cannot changes any parameters within the VAS Client. Extending or modifying a search permission can only be done with the PEAC user interface.

9. All actions are logged for auditing. Supervisors can access this audit logs.

The activity diagram below gives more details of a PO’s activity to accomplish a video search action.

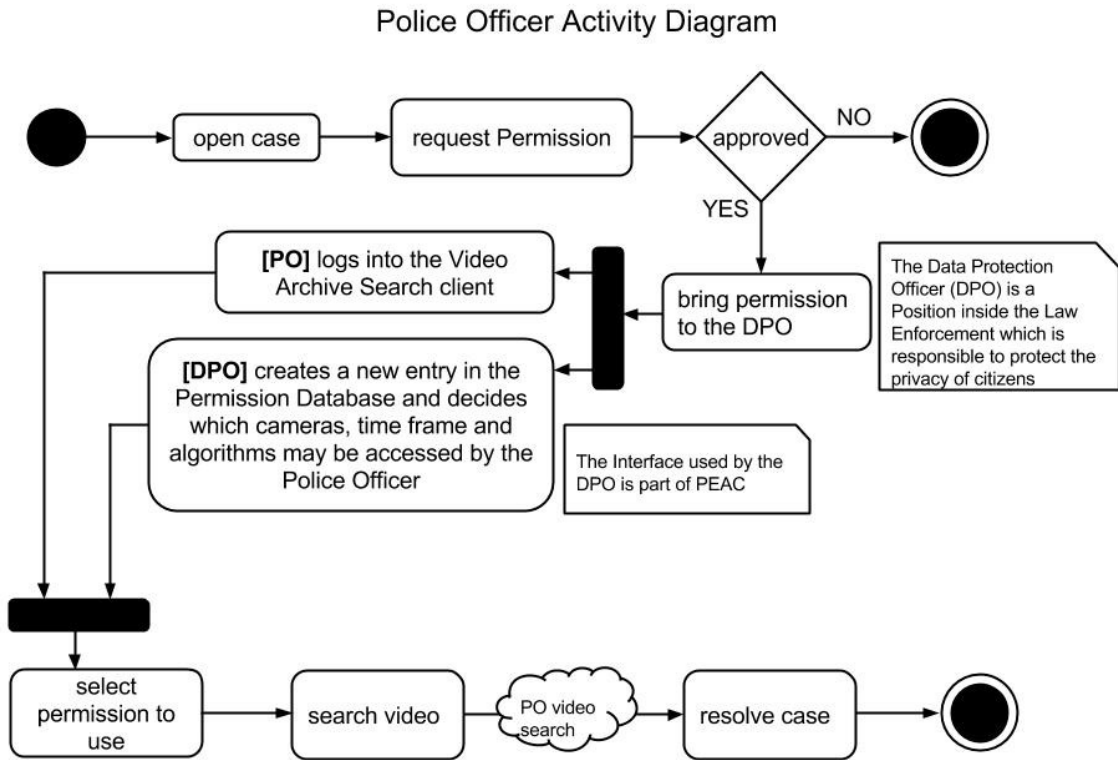


Figure 19: Police Officer activity diagram for VAS use case 1

The Data Protection Officer (DPO) opens a new case by creating a digital permission in the privacy preserving access control (PEAC).

A police officer (PO) can access and process his cases with the Video Archive Search (VAS). For this purpose, the VAS provides a user interface for the police officer to perform the approved and predefined search entered by the DPO.

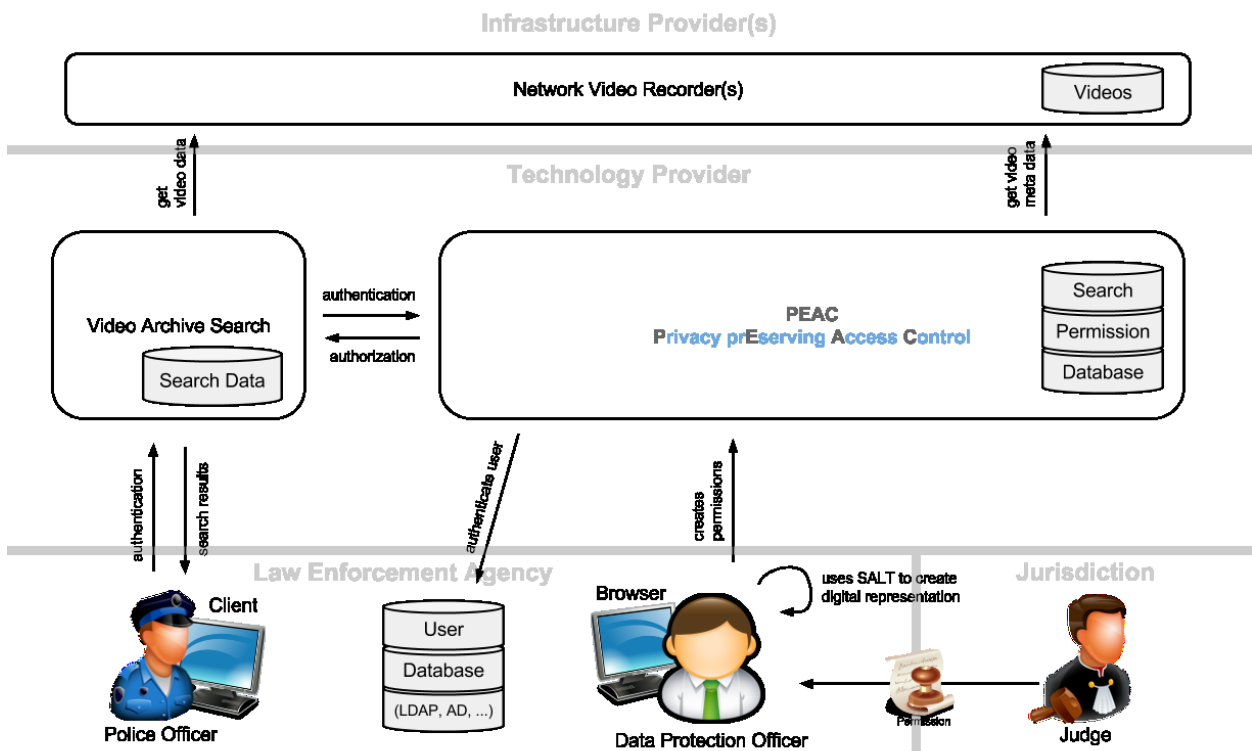


Figure 20: data flows at stake within use case 1

The system architecture follows the privacy by design principle as far as this is possible by a video surveillance application. This is guaranteed by careful handling of the data and selected algorithms. All modules access only the absolutely required data to perform the required task and do not save any unnecessary data or images.

From the external system view the PO authenticates himself to the user-interface of the VAS. The authentication is confirmed by the PEAC. Furthermore the PEAC provides the permissions and credentials for the NVR of the current PO to the VAS. When a search is started, video data are requested by the VAS from the NVR.

Internally the VAS consists of the user interface for the PO and the algorithm modules to perform the search. This modular design allows variable combinations and configurations of the algorithms to perform different search requests. For the Video Surveillance Lifecycle Management Use Case a set of algorithms has been chosen to demonstrate the search for generic persons in surveillance videos. These algorithms cover the following tasks:

- get video data from the NVR
- detect generic persons in the video data
- show thumbnail images for each detected person

Connection to NVR

The videos are requested on behalf of the PO, meaning that the required credentials are provided via the VAS to the NVR. The credentials are managed and provided by the PEAC. So it is possible for the NVR to, not only log that the VAS has accessed specific videos, but also who has given the order to do the search.

Generic person detector

This task searches for persons in the videos. The algorithm uses the generic shape of persons to detect persons in the images of the video. By using this method no specific information of persons are processed or stored. Even for detected persons no images of the person are stored in the VAS. The only data that are stored is the position of the detection and a reference to the video frame in the NVR.

Thumbnail images of detections

This module combines the video images and the result data from the detection step to show a thumbnail image of the detected persons. The thumbnail image is computed on-the-fly and not stored inside the VAS.

By consequently following the distributed approach, not only for user interactions (by separating the creation / opening of a case from the actual search task), but also for data management (by separating the storage of the image data and the search results saving the position only) the security of the whole system is increased.

4.2 Risks linked to use-case 1

The use case 1 main considered risks are linked to the potential use of IT (in the ISS sense, Information Security System) breaches to harm the system normal use. The threats considered are arising from malicious actions from the outside of the system, either from inside the system. These threats typically result in dramatically lowering the privacy level of the data, as unauthorized and unexpected disclosure is made possible.

These risks are here listed in the form of misuse cases. We use the following template to describe the misuse cases.

Name	(A simple, intuitive name that uniquely identifies the use case.)
Summary	(One or two sentences describing the interaction.)
Actor	(Who will be the attacker?)
Basic path	(The steps that the actors and the system go through to accomplish the goal of this use case.)
Preconditions	(Conditions that must be true before the use case can be performed.)
Post-conditions	(What will be true when the use case is completed?)

Note that we intentionally leave out the *countermeasures* in the misuse cases. The countermeasures will be a part of the privacy enhancing design.

The misuses cases are developed along two dimensions.

- Insider threat vs. outsider threat

- Privacy threats on confidentiality, integrity, and availability as proposed in CNIL privacy risk management methodology⁸.

Name	1.1 Attacker hacks into video archive search server and steals or modifies video data
Summary	An attacker with network access and/or physical access to the video archive search server obtains sufficient access rights to copy or modify either artifacts of the archive search data (e.g. video metadata) or raw video material cached at the video archive search server.
Actor	Insider, trusted third party with physical access, hacker
Basic path	An attacker with physical access (e.g. insider system administrator) or an attacker that gains physical access to the computer device or internal network by social engineering attacks like tailgating, or a trusted third party with access to the server (e.g. service personnel/contractor from HW/SW manufactures) may illegally copy video material to external data stores or modify the content of data. An attacker may inject malware into the system to help to reach its goal. Attackers that do not have physical access to the machine (either themselves or by a credulous administrator) will need network access to the video archive search server. In this case various attacks are possible e.g. malware sending the required material to the attacker, denial of service attacks that lead to unforeseen reactions of the server, video data may also be stolen or modifies in transit to e.g. the client or the network video recorder, and others.
Preconditions	Video data needs to be available and accessible at the video archive search server
Post-conditions	<ul style="list-style-type: none"> • Persons may unjustified suffer legal consequences if video material is modified • Persons that have committed a crime may not be found on video if material gets modified

Name	1.2 Attacker hacks into network video recorder
Summary	An attacker with network access and/or physical access to the network video recorder gets sufficient access rights to copy or modify raw video material in the NVR.
Actor	Insider, trusted third party with physical access, hacker
Basic path	Attackers with physical access (insiders e.g. system administrators) or attackers that gain physical access to the machine with social engineering attacks like tailgating or trusted third parties with access to the server (e.g. service personnel from HW manufactures) may illegally copy or modify video material to external data stores or they may install malware. Attackers that do not have physical access to the machine (either themselves or by a credulous administrator) will need network access to the

⁸ CNIL, Methodology for privacy risk management, <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf>

	network video recorder. In this case various attacks are possible e.g. malware sending the required material to the attacker, denial of service attacks that lead to unforeseen reactions of the server, video data may also be stolen or modifies in transit to the video archive search server.
Preconditions	Video data needs to be available and accessible at the network video recorder
Post-conditions	<ul style="list-style-type: none"> • Persons may unjustified suffer legal consequences if video material is modified • Persons that have committed a crime may not be found on video if material gets modified

Name	2. Hacker launches a DoS attack against VAS or NVR server
Summary	External attacker carries out a Denial of Service (DoS) attack to cause VAS or NVR server unresponsive to normal request
Actor	External attacker
Basic path	An external attacker with direct connection to the VAS or NVR over the Internet carries out a (maybe distributed) denial of service attack. The goal of this attack is to make the video archive search or the network video recorder unresponsive. If attacker has physical access to the server actions may also be carried out that lead to service unresponsiveness.
Preconditions	<ul style="list-style-type: none"> • NVR or VAS is exposed to the Internet • No DoS attack countermeasures in place
Post-conditions	NVR or VAS is unresponsive

Name	3. Hacker hacks and modifies search permission database
Summary	An attack illegally modifies the search permission database to either elevate or reduce the privilege of a search action specified in a permission.
Actor	External attacker
Basic path	<ul style="list-style-type: none"> • An attacker may be interested to modify a search permission stored in the permission database • The attacker elevates its access privilege right to the permission DB • The attacker modifies permission DB directly due to weaknesses in DB security settings and/or web client
Preconditions	<ul style="list-style-type: none"> • Permissions need to be stored in the DB • Search permission database can be accessed remotely • Security measures at permission DB are not sufficient to protect against unauthorized access
Post-conditions	The scope of the video archive search action does not conform with the permission issued by the judge

Name	4. Someone fakes a permission from the judge
------	--

Summary	A permission is faked by an attacker
Actor	<ul style="list-style-type: none"> Employee of court Employee of law enforcement agency
Basic path	A permission is faked by an attacker with the goal that either an unjustified archive search can be performed or additional restrictions are added to the permission that the archive search won't be able to find the criminal
Preconditions	No or insufficient integrity checks for permissions
Post-conditions	An unauthorized video archive search is performed, or a video archive search is under-performed.

Name	5. Man-in-the-middle between NVR and VAS or VAS and client
Summary	Man-in-the-middle attack between NVR and VAS or VAS and web client
Actor	External attacker
Basic path	<ul style="list-style-type: none"> Man-in-the-middle sniffs at data traffic between NVR and VAS or VAS and web client. The attacker may also modify data.
Preconditions	<ul style="list-style-type: none"> The communication is not encrypted If the communication is encrypted, the communication parties do not verify the digital certificates of their correspondents If the communication is encrypted and the attacker forged a certificate that is accepted by the correspondents
Post-conditions	Video data may be copied and/or modified

Name	6. Social engineering to steal login credentials (DPO or PO)
Summary	An attack uses social engineering to obtain login credentials from a DPO or PO
Actor	<ul style="list-style-type: none"> External Attacker Colleague of DPO or PO with insufficient access rights
Basic path	Actor undertakes social engineering attacks against DPO or PO with the goal to get DPOs or POs access credentials to the system
Preconditions	<ul style="list-style-type: none"> DPO and PO are prone to social engineering No two-factor-authentication in place
Post-conditions	The attacker can access the system which seriously comprises security and privacy controls

Name	7. Hacker exploits a weak client implementation to steal login credentials of users
Summary	An attacker exploits a weak client implementation to steal login credentials of users
Actor	External attacker

Basic path	<ul style="list-style-type: none"> Client is used for access to VAS server and permission DB An attacker may use critical vulnerabilities in the client implementation to gain access to the server The attack may even be able to retrieve passwords or other user credentials from the client
Preconditions	<ul style="list-style-type: none"> Weak client implementation Client unpatched against vulnerabilities
Post-conditions	Loss of login credentials

Name	8. A PO performs video search functions or accesses video sources beyond his investigation duty
Summary	Police officer exceeds his authority to perform video search actions or access video data beyond the purpose of his specific investigation case
Actor	Insider (police officer)
Basic path	<ul style="list-style-type: none"> There is weakness in the design and implementation of VAS access control, due to factors such as mistakes or ambiguities in access control policy definition, or a conceptual error or a bug in the design and implementation. Due to the weakness, the police officer is able to exceed his authority and perform unauthorized video archive searches.
Preconditions	Errors in access control system
Post-conditions	Police officer may use search results for various purposes beyond his duty, and breach privacy

Name	9. A PO colludes with DPO
Summary	PO colludes with DPO to exceed authorized power
Actor	Police officer and data protection officer
Basic path	Police officer or data protection officer has interest in performing a video archive search without legal permission. They may also be interested in hiding results (DPO configures search accordingly)
Preconditions	No integrity check mechanisms of permission in DB with search permission of judge
Post-conditions	Law enforcement agency misuse its power and does not comply to privacy and data protection regulations and rules

Name	10. DPO wrongly interprets the video search permission and gives too much access rights to a PO
Summary	DPO unintentionally configures video archive search actions which gives PO too much access right
Actor	Data protection officer of law enforcement agency
Basic path	<ul style="list-style-type: none"> DPO misinterprets search permission by judge and give PO too much

	access rights <ul style="list-style-type: none"> • DPO makes a mistake in entering access rights for PO
Preconditions	<ul style="list-style-type: none"> • No clear mechanisms in place to interpret and transform paper-based search permission to VAS configurations • No integrity check mechanisms of permission in DB with search permission of judge
Post-conditions	Too much access rights for PO may lead to illegal (intentionally or unintentionally) video archive searches by PO

Name	11. A PO retains video data that is not relevant to his investigation
Summary	Police officer retain video data from VAS beyond its allowed retention period and purpose
Actor	Insider (Police officer)
Basic path	<ul style="list-style-type: none"> • At some point the police officer has access to video material which is not relevant for his investigation (maybe due to too many false positives in video archive search). • Police officer either copies data on external storage device, network storage, or takes pictures with his photo camera
Preconditions	PO has the possibility to store video material outside of the system
Post-conditions	PO is in possession of video data that is beyond its retention period and purpose

The diagram summarizes the above misuse cases.

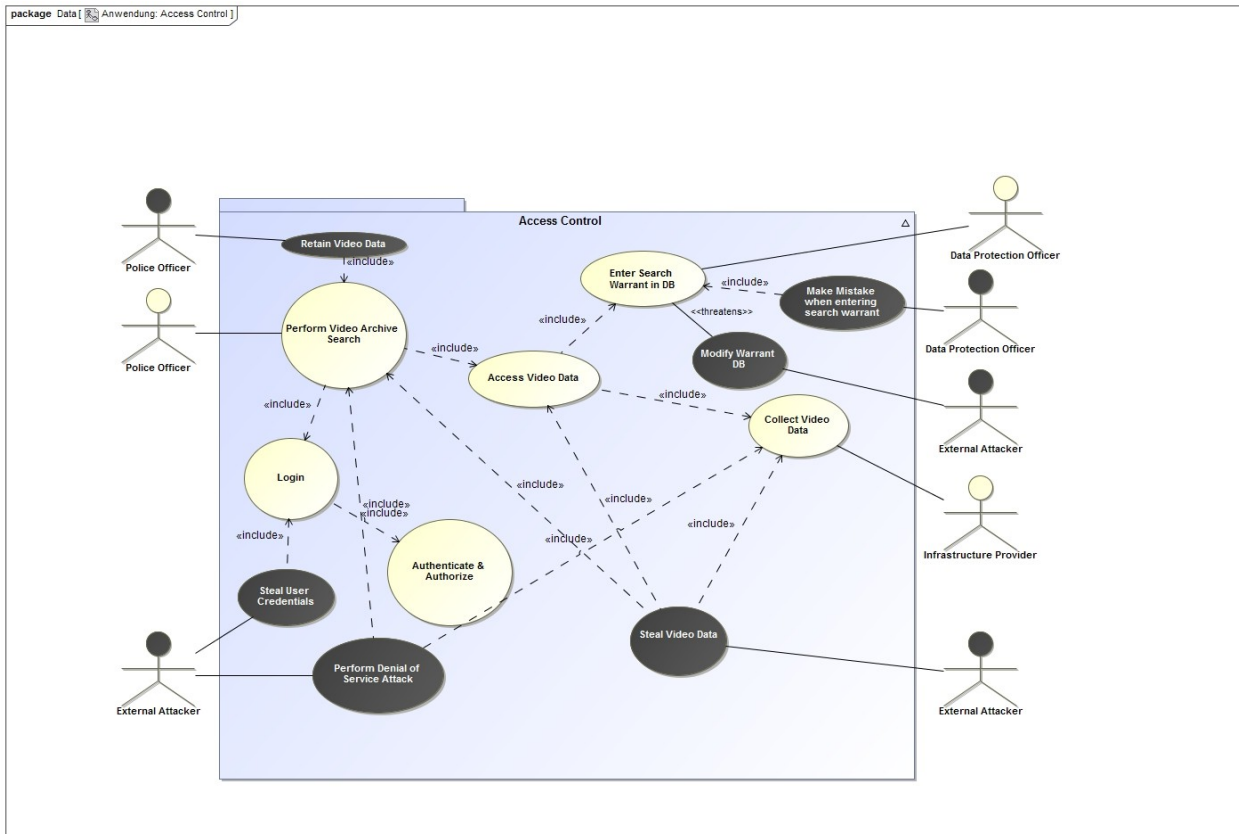


Figure 21: graphical summary of VAS use case 1 misuse cases

5 Specification of VAS use-case 2 and associated risks to privacy and accountability

5.1 Specification of VAS use case 2: accountability of operators

Short Description of the proposed use-case:

This use case aims at demonstrating the use of accountability mechanisms dedicated to the use of the system, especially:

- Tools enabling to log the operators actions
- Tools enabling to date the latest video-recordings reachable in a system.

An imaginary scenario is proposed to underline the importance of the accountability of the operator actions. The basic idea is to demonstrate how an accountability request performed by a court about surveillance operator actions can be handled within a privacy- and accountability by design system.

The case described is basically the need to prove that a crime that was committed within the field of a surveillance camera was not seen by an operator, or, if it had been seen, to bring information about the operator(s) that might have been aware of the crime (e.g. his/their identity).

The importance of the accountability of the operators could be brought forward using other scenarios, such as this one, corresponding to an actual privacy threats: a citizen makes a complaint about a video he found on the internet, on which he is recognizable. This video is clearly issued from a video-surveillance camera displayed on a screen itself filmed, probably using a personal mobile phone. In this concrete case, the accountability of the operator actions is also at stake as there is a strong chance that one is implied in the crime.

Main actors of the proposed use-case:

- Victim
- Judge
- LEA
- Operator
- DPA

Aims of the proposed scenario:

To provide and demonstrate an access control system to video management system, featuring authentication capabilities and authorization capabilities (applicable both to live view of videos and to their replay). Based on this access control module, to provide a logging and auditing tool of operator actions, and to demonstrate the use and interest of this auditing tool to process accountability-related requests about the operators' actions.

Note that the scenario that is proposed below (based on a criminal case) is intended to demonstrate the capabilities and benefits of the use of operators' accountability mechanisms. During the concrete demonstration, as recorded video footages will be used, the demonstration will be based upon a different case (depending on the content of the available video footages). The aim of the scenario will remain to demonstrate the power of auditing and logging tools (based on access controls to the recordings) to prove that a video sequence has been or not displayed on an operator workstation or video-wall, which is a very strong accountability statement.

The demonstration will be mainly performed using technical tools developed in the frame of the PARIS project within the Network Video Recorder (by Thales) and within the Video-Archive Search engine (by AIT), both sub-systems being bridged together by the 2 partners.

This demonstration features mainly the accountability of the actions of the operators using technical means. Other means (not considered there), based on procedures and trainings enforced within the organization responsible for the operators may also allow to higher the global privacy- and accountability- protection linked to the use of the surveillance system.

Preconditions of the proposed use case:

- Legal recording permission for IP
- Accepted viewpoint for involved cameras by DPA
- Accepted operators actions auditing strategy by DPA
- A crime is committed and a subpoena exists

Scenario description:

The goal of this use case is to illustrate the interest of logging the operator actions.

Tabasco-City is equipped with a wide video surveillance system, featuring a very large number of cameras (10000). The surveillance of the city is performed by hundreds of operators using this system in conjunction with communication means (citizens, responders). The organization of the supervision is very complex as:

- Some operators perform the supervision from local police district buildings,
- Some operators perform the supervision from city-wide police headquarters,
- Some operators belong to the fire fighters organization,
- Some operators use sometimes the systems mainly for road traffic supervision.

Moreover, Tabasco-City is very well illuminated enabling a permanent supervision (day and night). A single operator position is used by several persons rotating.

The Tabasco city has nevertheless purchased a privacy and accountability –by design proven system, featuring advanced operators management policy. Moreover, a strict enforcement of the maximum retention period for video recordings is performed by the system (21 days retention period for some cameras, no recording at all for some others).

A woman was injured last week in a car hijacking in one street downtown. The judge required an extract of available video-footages from the place where the crime occurred (use case I). From this footage it appeared that images of the crime from a distant large angle camera were available (no sufficient details to identify the thief), but that nobody had neither noticed the problem live and given the alert, nor tried to focus the other cameras available within the zone to collect precious evidence information about the on-going crime. This appears surprising, to the judge, but also to the population.

The judge decides to request the DPA administrator to perform an extract of the log bases of the system to understand:

- If someone (and who) was viewing the camera with clear crime images,
- What the operators in charge of the zone were watching at this precise moment.

It finally appears that the operators were all watching other cameras at this time. The video footages have shown that many other incidents that happened in the same time focused unfortunately their attention.

Technical description

Details about the login and audit of operators actions in the within the video-surveillance ecosystem

The figure below (Figure 22) depicts the main external system interfaces that are implied in this use case. The external interfaces identified in green are the interfaces used by operators to perform their actions related to the video streams (real-time or recorded, with or without processing). The external interface identified in red is the one used to perform some enquiries about the operators' action, using an auditing tool.

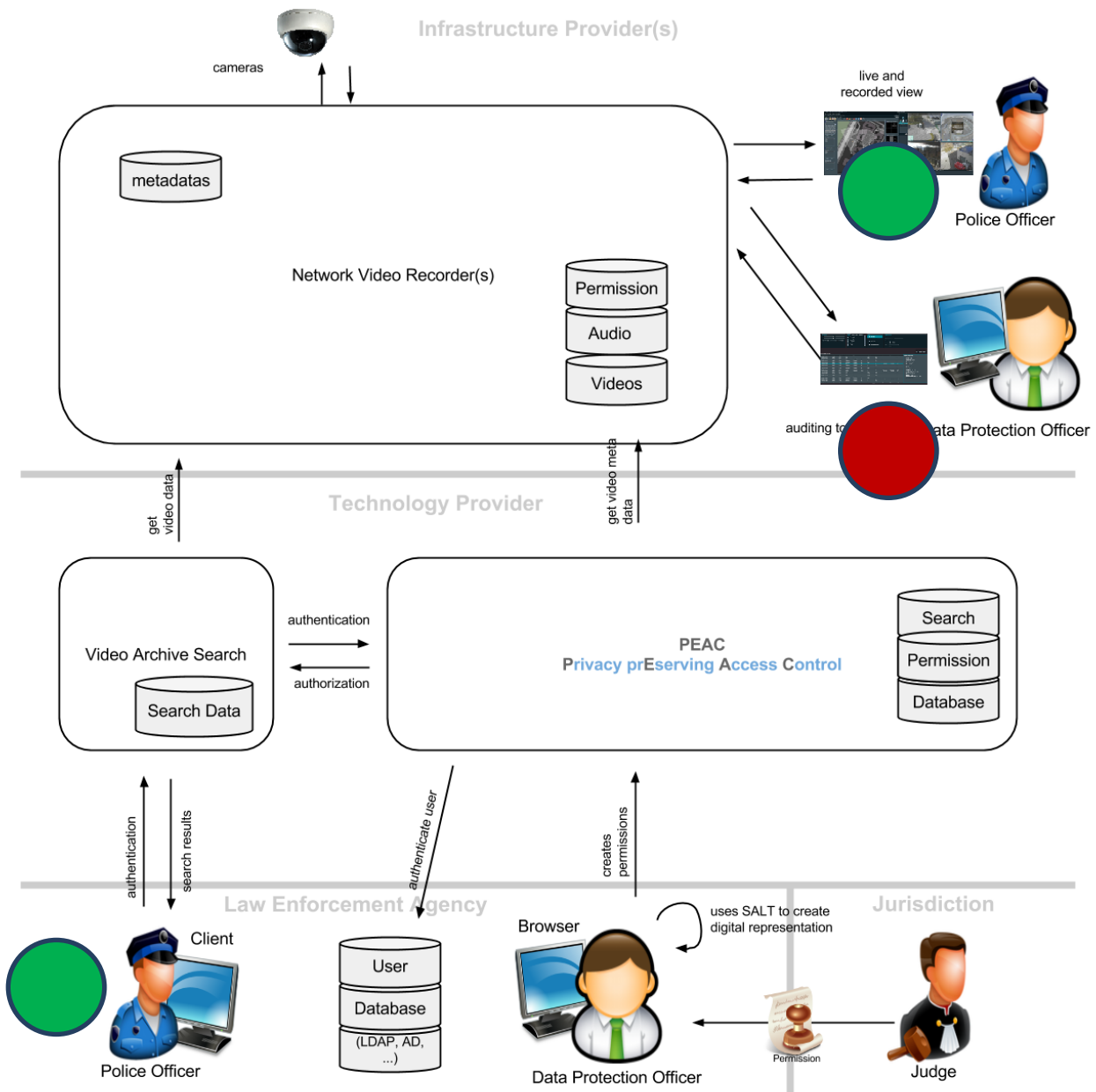


Figure 22: illustration about the auditing process about the operators' actions

In the proposed demonstration system, 2 main external interfaces are used by operators to interact with the video streams:

- The standard interface directly linked to the video-management system, enabling to select cameras, to display live streams, to display recorded streams and to export streams of interest out of the system using dedicated tools and following well-defined procedures. These are the basic capabilities of any video-management system (embedding a network video recorder). Many other supporting capabilities may be included within this subsystem (pre-sets and cycles management, geographical navigation, use of mobile devices featuring a camera, configuration related capabilities),

- The interface of the VAS (Video Archive Search) module, that is particularly at stake within the VAS use-case 1 (described from p. 73). This interface enables to browse the videos using powerful analytics algorithms, which allow to higher the performance of the search operation, both providing better hit ratio, and by accelerating the searches.

A typical operator interface of the video-management system is reproduced on the figure below (Figure 23).

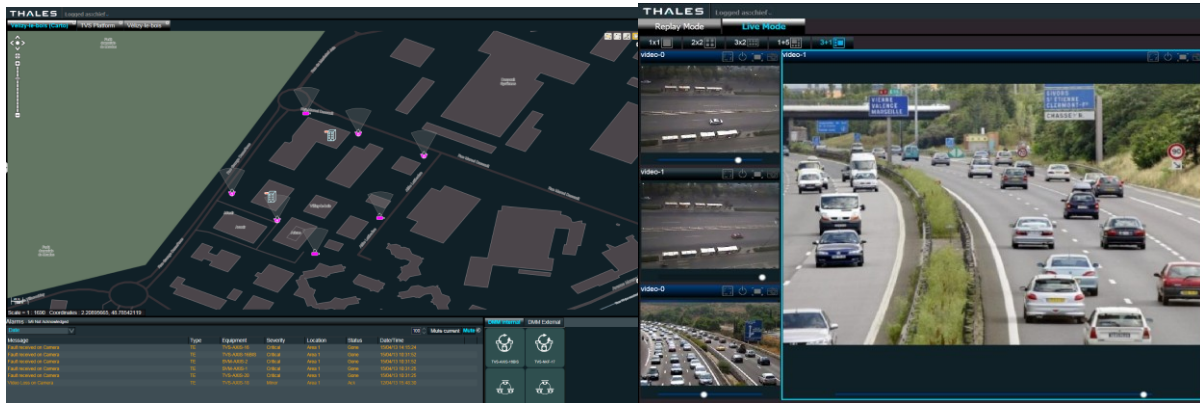


Figure 23: illustration about live and recorded video management system

This figure depicts a 2-screen HMI: the left HMI is dedicated to camera selection, geographical browsing, and complex search and commands. The right screen of the HMI is dedicated to the display of the live and recorded videos.

The demonstration system that is developed and integrated within the scope of the PARIS project is likely to embed only the right HMI screen, as the cameras will be simulated using privacy-free recordings (the video footage that will be used are subparts of the ILIDS library). These recordings will be played from the NVR as if they were issued from real cameras (the NVR acts as a camera simulator).

The operator interface to the second HMI that allows to manipulate videos is described in the part of this document dedicated to the use case 1 (§ 4.1). Basically, it mainly proposes capabilities to intelligently search and access recorded streams. Intelligence is provided by advanced analytics allowing to automatically detecting patterns within the video streams. These patterns range from simple movement detection (with or without attributes such as speed, size, direction, duration), to advanced ones (such as person detection and extraction).

A given video-surveillance system can use several operator stations of each kind simultaneously. In our advanced system, any operator who performs some surveillance actions using the system has first to log. This login is personal and is linked to the operator himself, and not to the hardware (the computer used to host the operator station).

The authentication of the operators is recorded together with their actions at 2 levels of the system (and with potentially many other parameters such as location, time):

- Within the PEAC (Privacy pReserving Access Control) module, only for the actions performed through the VAS interface,
- Within the NVR (Network video recorder) for the action performed through the VAS interface and for the action performed using the Video-Management System interface.

The records performed are often referred to as “logs” or “traces”. In real systems, they can themselves be protected (full encryption, encryption of the identity of the persons, specific access right policy).

The auditing tool developed in the field of the PARIS project is a BI (Business Intelligence) system that relies on the NVR logs. It allows performing multiple-field requests to retrieve records of interest from the records base (time, camera, position, action).

The figures below depict the operator interface for this type of auditing system. This interface allows both to formulate the request, and to browse the recordings corresponding to the request.

Choose search criteria

Synthesis of the chosen criteria

Remove every search criteria

Run the search with the chosen criteria

Result of the search

Date & time	Originator	Log type	Log category	Type	ID	Operator	Status
16/10/2012 17:44:52	App 5	CRP	New	Event type 0	Command_20_22	user1	Not yet
16/10/2012 17:44:52	App 11	EV7	Raw	Event type 0	Event 2	-	-
16/10/2012 17:44:52	App 5	ALB	Adressat	Alarm type 0	Alarm_M_00	user2	-
16/10/2012 17:44:52	App 2	EV7	Raw	Event type 0	Event 0	-	-
16/10/2012 17:44:52	App 8	EV7	Raw	Event type 0	Event 4	-	-
16/10/2012 17:44:52	App 2	EV7	Raw	Event type 0	Event 2	-	-
16/10/2012 17:44:52	App 2	GBB	Custom 10	-	-	-	-
16/10/2012 17:44:52	App 2	CRP	Update	-	Command_M_0	-	Running
16/10/2012 17:44:52	App 5	EV7	Raw	Event type 0	Event 1	-	-
16/10/2012 17:44:52	App 2	GBB	Custom 10	-	-	-	-
16/10/2012 17:44:52	App 3	CRP	Update	-	Command_M_00	-	Running
16/10/2012 17:44:52	App 4	EV7	Raw	Event type 0	Event 0	-	-
16/10/2012 17:44:52	App 11	ALB	Adressat	Alarm type 0	Alarm_M_07	F_JA	-
16/10/2012 17:44:52	App 8	EV7	Raw	Event type 0	Event 2	-	-
16/10/2012 17:44:52	App 11	CRP	New	Event type 0	Event 2	user2	-
16/10/2012 17:44:52	App 11	EV7	Raw	Event type 0	Event 2	-	-
16/10/2012 17:44:52	App 8	EV7	Raw	Event type 0	Event 4	-	-
16/10/2012 17:44:52	App 2	ALB	Adressat	Alarm type 1	Alarm_M_04	user2	-
16/10/2012 17:44:52	App 3	GBB	Custom 10	-	-	-	-
16/10/2012 17:44:52	App 3	ALB	Adressat	Alarm type 2	Alarm_M_2	-	MP_JA
16/10/2012 17:44:52	App 4	EV7	Raw	Event type 0	Event 0	-	-
16/10/2012 17:44:52	App 11	EV7	Raw	Event type 0	Event 1	-	-
16/10/2012 17:44:52	App 3	EV7	Raw	Event type 0	Event 1	-	-
16/10/2012 17:44:52	App 5	ALB	Adressat	Alarm type 0	Alarm_M_20	MP_JA	-
16/10/2012 17:44:52	App 11	ALB	Adressat	Alarm type 0	Alarm_M_8	MP_JA	-
16/10/2012 17:44:52	App 11	EV7	Raw	Event type 0	Event 0	-	-

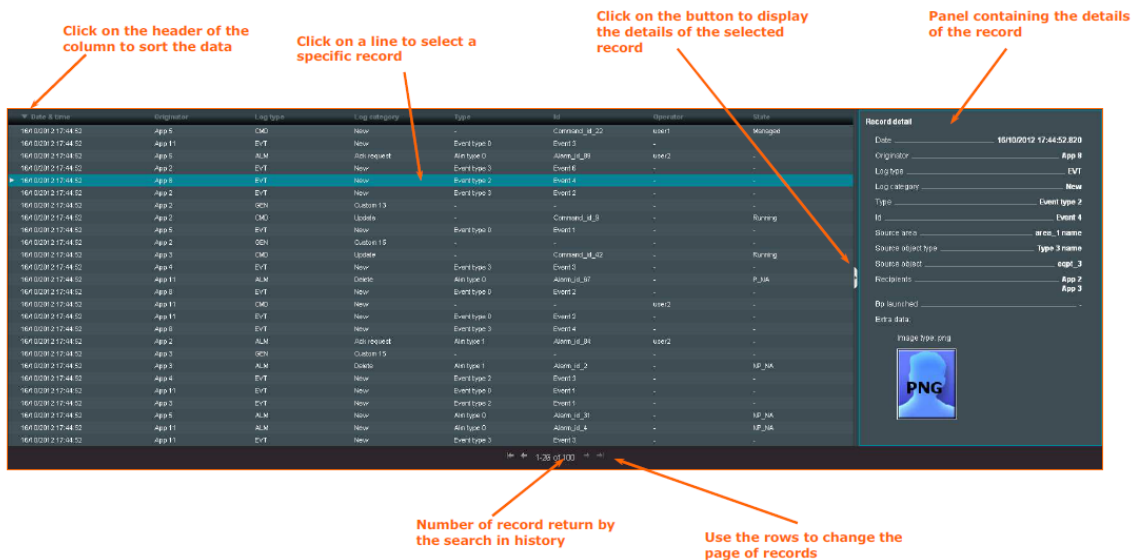


Figure 24: illustration about the auditing tools for the operators' actions

In the field of the VAS use-case 2, the criteria for the search will mainly be the camera of interest identifier, and the time and date of the occurrence of the prosecuted crime.

5.2 Privacy and accountability risks linked to use-case 2

As for the use case 1, risks are here listed in the form of misuse cases. We use the following template to describe the misuse cases.

The risks identified here, because of the thematic treated, are mainly related to the accountability of the operators, and more generically to the organisation that is responsible for the operators and for the exploitation of the system.

Name	(A simple, intuitive name that uniquely identifies the use case.)
Summary	(One or two sentences describing the interaction.)
Actor	(Who will be the stakeholders?)
Basic path	(The steps that the actors and the system go through to accomplish the goal of this use case.)
Preconditions	(Conditions that must be true before the use case can be performed.)
Post-conditions	(What will be true when the use case is completed?)

Identified accountability risks

Name	Accountability of organisations in a multi-agencies system
Summary	Several agencies use the system. An action performed on the system is questioned (orientation of a camera in specific direction, monopolization of

	a camera, abnormal export of a video file) is questioned: which is the organisation who performed the action?
Actor	Agencies using the system physically likely to have performed the action.
Basic path	Use of standard capabilities of the VAS or of the VMS in a complex multi-agencies, multi-operators surveillance ecosystem
Preconditions	An access control mechanism is used upon the surveillance system. An abnormal usage of the system is detected, even if not likely to be classified as criminal.
Post-conditions	The organisation responsible for the malfunction is identified

Name	Accountability of the organisation about the completeness of the surveillance
Summary	A complex infrastructure or site, or town is monitored using a video-surveillance system. Being large, the surveillance is performed by several operators with separated geographical zones. For any reason, it is requested to show that at a given instant in time the whole infrastructure is supervised.
Actor	The operators of the video-surveillance system, the internal or external authority raising a request for evidence that the site or infrastructure is continuously extensively monitored
Basic path	Typically a doubt about the completeness of the surveillance linked to non-detection of events or abnormalities
Preconditions	Internal or external authority request evidence that there is no spatial or temporal lack within the surveillance
Post-conditions	Answer to the request for evidence

Name	Accountability of the operator and organization towards the non-authorized diffusion of video footages
Summary	Video footages internal to an organization (public or private), collected using a video-surveillance system, are found outside of the system: typically on the internet.
Actor	Operator, citizen subject to surveillance
Basic path	Complaint from a citizen that an unexpected and unauthorized video footage where he is visible is found on the net, harms both his privacy and himself
Preconditions	Formal or informal complaint about video footages
Post-conditions	Identification of all the operator that have either exported either displayed the images

Name	Accountability of the operator and/or organization for non-authorized production of a video export
Summary	A video export is found with no legitimate ground for existence
Actor	An operator performing an export outside of the scope of an authorized request.
Basic path	A video export is found without credential authorizing its production
Preconditions	Identification of the operator responsible for the production of the export, and therefore of the organization in responsibility if the action
Post-conditions	Identification of the operator and organisation responsible for the export

Name	Accountability of operator about reaction to a crime
Summary	A crime is reported, it happened under a camera but was not reported by any operator of the video-surveillance system
Actor	Operators, persons implied in the crime, persons implied in the crime prosecution
Basic path	A crime happens. An official or unofficial complaint is issued. An investigation is performed.
Preconditions	The crime was or was likely to be filmed by a video surveillance camera itself likely to be monitored real-time by one or several operators
Post-conditions	Identification of the operators (if any) who displayed the criminal scene

6 Conclusion

This deliverable of the WP5 “Using SALT for video-surveillance data lifecycle management” achieves two main goals: the first goal is the refinement of the description of the use cases from technical and operational points of views, including the identification of the main risks at stake regarding these use cases, especially regarding privacy and accountability, but also regarding security. The second goal of the deliverable is to specialize the contents of the SALT framework for the use cases related to video-surveillance. This has been done, by providing example references (atomic contents of the SALT framework, managed by the related tools, namely the SFMT, SALT Framework management tools), within the 3 pillar dimensions covered by the SALT approach to security, privacy and accountability: the Socio-Ethical axis, the Legal axis and the Technical axis.

The references provided in this document are not pursuing the goal of completeness, but rather exemplify the type of information that can be embedded in the SALT framework. Also, the usage philosophy and guidelines for the use of the SALT Framework Management Tools, arising from the works realized and those ongoing in the WP3 “SALT frameworks Management Tools” and WP4 “SALT compliant processes” have been summed up. Both pieces of information, about contents of the SALT framework, one side, and processes regarding their use, the other side, enable to figure out more precisely how the SALT approach globally allows to actually handle multi-disciplinary information and constraints about surveillance systems. It also points out that, even based on best of the breed IT tools applied to knowledge storage, the balanced decision about a surveillance system, between privacy/accountability and security results from a human decision. The SALT approach can be seen as an effective set of tools that allows informed choices about surveillance systems, these choices being themselves accountable and possibly collaborative thanks to this tool. The balancing of potentially multi-direction constraints results from this choice.

The next actions that are to be carried in the field of the WP5 are the filling of the SALT tools with the references presented in this deliverable, potentially augmented with some other references, and to show a simple concrete balance between security and privacy arise regarding the video-surveillance life cycle management, with the understanding that the balance performed is not unique. Some of the concrete privacy / accountability mechanisms at stake within this use case will be demonstrated on a concrete technical video-surveillance chain.

7 References

*[The content is indicative and subject to change through the writing process of this deliverable.]

[1] Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance, Version consolidée au 16 mars 2011 (executive decision from 3 of August 2007, for the definition of technical standards of video-surveillance systems, consolidated version from 16 of March 2011). Available e.g. at

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000649127>

[2] enquête “les Français et la video-surveillance” (survey about French people and video-surveillance), IPSOS Public affairs/ CNIL March 2008. Available e.g. at

http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CC8QFjAC&url=http%3A%2F%2Fwww.cnil.fr%2Ffileadmin%2Fdocuments%2FLa_CNIL%2Factualite%2FCNIL-sondagevideosurveillance.pdf&ei=WmGIVlyLPMz0UJeggpAO&usg=AFQjCNFc-xZ_Ro3k-vWL1SI1Vylwoh9v9w&sig2=ixJhYQ5J7TK9pdRQanhYEA&bvm=bv.81456516,d.d24&cad=rja

[3] LOI INFORMATIQUE ET LIBERTES

ACT N°78-17 OF 6 JANUARY 1978

ON INFORMATION TECHNOLOGY, DATA FILES AND CIVIL LIBERTIES

AMENDED BY THE FOLLOWING LAWS:

ACT OF 6 AUGUST 2004 RELATIVE TO THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

ACT OF 13 MAY 2009 RELATIVE TO THE SIMPLIFICATION AND CLARIFICATION OF LAW AND LIGHTER PROCEDURES

LAW NO.2009-526 DATED 13/05/2009

ORGANIC LAW NO.2010-704 DATED 28/06/2010

LAW NO.2011-334 DATED 29 MARCH 2011 RELATIVE TO THE DÉFENSEUR DES DROITS

ORDINANCE NO.2011-1012 DATED 24/08/2011

[4] directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

[9] ISO/IEC 29100:2011(E) standard: Information technology, security techniques, privacy framework

[10] ISO/IEC 24760-1:2011(E) standard: Information technology, security techniques, a framework for identity management