



# PrivAcy pReserving Infrastructure for Surveillance

## Deliverable D5.3

### Video Surveillance Lifecycle Management Use Case

Project: PARIS  
Project Number: SEC-312504  
Deliverable: D5.2  
Version: v0.5  
Date: 21/07/2015  
Confidentiality: Public  
Authors: Mathias Bossuet (Thales)  
Timothe Aeberhardt (Thales)  
Francisco Jaime (UMA)  
Zhendong Ma (AIT)  
Stephan Veigl (AIT)  
Daniel Hovie (AIT)  
Claire Gayrel (U Namur)  
Fanny Coudert (KU Leuven)  
Lina Jasmontaite (KU Leuven)



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

# Table of Contents

<b>DOCUMENT HISTORY .....</b>	<b>4</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>ABBREVIATIONS AND DEFINITIONS.....</b>	<b>7</b>
<b>1 INTRODUCTION .....</b>	<b>9</b>
<b>2 SALT FRAMEWORK SPECIALIZED FOR VIDEO-SURVEILLANCE .....</b>	<b>10</b>
<b>2.1 SALT CONTENTS: QUESTIONNAIRES .....</b>	<b>11</b>
<b>2.2 SALT CONTENTS: REFERENCES.....</b>	<b>12</b>
2.2.1 References template .....	13
2.2.2 References list .....	15
<b>2.3 SALT CONTENTS: TAXONOMIES .....</b>	<b>18</b>
<b>3 REFINED DESCRIPTION OF THE ARCHITECTURE OF THE MOCK-UP VIDEO-SURVEILLANCE SYSTEM.....</b>	<b>21</b>
<b>3.1 GENERAL ARCHITECTURE OF THE SYSTEM.....</b>	<b>21</b>
<b>3.2 DETAILED ARCHITECTURE OF THE NVR AND PRIVACY-ENHANCING COMPONENTS AND DEVELOPMENTS .....</b>	<b>22</b>
3.2.1 Presentation of the Thales NVR .....	22
3.2.2 Enhancements and developments.....	23
3.2.3 Ideas for further improvements.....	27
<b>3.3 DETAILED ARCHITECTURE OF THE VAS AND PRIVACY-ENHANCING COMPONENTS AND DEVELOPMENTS.....</b>	<b>27</b>
3.3.1 Video Analytics System.....	27
3.3.2 Privacy prEserving Access Control (PEAC).....	30
<b>4 ILLUSTRATED APPLICATION OF SALT PROCESSES AND TOOLS TO THE VIDEO-SURVEILLANCE USE CASE .....</b>	<b>36</b>
<b>4.1 OVERVIEW ABOUT THE USE OF THE SALT TOOLS .....</b>	<b>37</b>
4.1.1 System proposer SALT tools use description .....	37
4.1.2 System designer SALT tools use description .....	38
4.1.3 System developer SALT tools use description.....	40
4.1.4 Other stakeholders potential use of the tools .....	41
<b>4.2 SPECIFICITIES OF THE USE-CASE 1 .....</b>	<b>41</b>
4.2.1 Use case scenario .....	42
4.2.2 Privacy-preserving video analytics system.....	43
4.2.3 Reference / concern .....	47
<b>4.3 SPECIFICITIES OF THE USE-CASE 2 .....</b>	<b>47</b>
4.3.1 Use case scenario .....	48
4.3.2 Example main outputs from SALT tools and processes .....	50
4.3.3 Log and audit tools for enhanced accountability and their use.....	53
<b>5 CONCLUSION .....</b>	<b>55</b>

---

<b>6</b>	<b>REFERENCES .....</b>	<b>56</b>
<b>7</b>	<b>ANNEX A: ADVISE PROJECT PIA.....</b>	<b>57</b>
7.1	GENERAL AND TECHNICAL DESCRIPTION .....	57
7.2	DESCRIPTION OF INFORMATION FLOWS, INCLUDING PERSONAL DATA.....	58
7.3	ADDENDUM: QUESTIONS RELATING TO THE RECORDING ITSELF.....	59
7.4	RISKS IDENTIFICATION.....	60
7.4.1	Risks related to ethics.....	60
7.4.2	Risks related to the right to privacy .....	61
7.4.3	Risks related to the right to the protection of personal data .....	62
7.4.4	Risks related to other fundamental rights .....	62
7.5	RISK ASSESSMENT.....	63
7.5.1	Controls already implemented.....	63
7.5.2	Risk mitigation .....	63
7.6	RECOMMENDATIONS FOR THE DESIGN OF THE COMPONENT/SYSTEM .....	64
<b>8</b>	<b>ANNEX B: SALT REFERENCES FOR THE VIDEO-SURVEILLANCE USE CASE .....</b>	<b>65</b>
8.1	INTRODUCTION .....	65
8.2	SALT REFERENCES TEMPLATE.....	66
8.3	SALT REFERENCES FOR THE VIDEO-SURVEILLANCE USE CASE .....	69
8.3.1	Legal SALT references for the video-surveillance use-case.....	69
	LawFrance.1 .....	76
	LawFrance.2 .....	76
8.3.2	Socio-Ethical references for the video-surveillance use-case.....	104
8.3.3	Technical references for the video-surveillance use-case .....	110
8.4	REUSE POSSIBILITIES OF THE WP6 REFERENCES.....	130
<b>9</b>	<b>APPENDIX C: MAPPING OF ISO PRINCIPLES AND SALT LEGAL TOPICS.....</b>	<b>132</b>

## Document History

Version	Status	Date
V0.1	First version, with table of contents (Thales)	21/04/2015
V0.23	Evolved and fully structured version (Thales)	02/06/2015
V0.3	Augmented version (Thales)	15/06/2015
V0.4	Integration of AIT and UMA contributions	23/06/2015
V0.5	Augmented version delivered as DRAFT	29/06/2015
V0.6	Finalisation with new contributions from Thales and AIT	15/07/2015
V1.0	Version reviewed, delivered to the commission	21/07/2015

Approval		
	Name	Date
Prepared	Maria-Cinta Saornil Gomez (Visual Tools)	20/07/2015
Prepared	Christophe Jouvray (Trialog)	20/07/2015
Prepared		
Authorised		
Circulation		
Recipient	Date of submission	
Project partners	21/07/2015	
European Commission	21/07/2015	

## Executive Summary

This document comes in the line of the D5.1 and D5.2: it bridges the technical and operational description of the video-surveillance use-case with privacy-by-design and accountability-by-design concerns and explains how these concerns are managed using the SALT tools and processes.

Two use cases are considered, both applied to a video-surveillance system used by the police for forensics operation over video feeds from cameras placed in public spaces. A first use case is dedicated to the demonstration of privacy by design concrete implementation thanks to the SALT tools and processes; the second use case meets the accountability-by-design perspective.

The 2 use-cases are described from the technical and operational points of view; the application and expected results from the SALT tools and processes are described, alongside with SALT contents dedicated to video-surveillance systems.

The SALT tools, methodology and contents are this way exemplified and linked to the privacy and accountability preserving mechanisms that have been developed by AIT and Thales in their common demonstration.

The next deliverable will be based on these grounds and will focus on the concrete manipulation of the SALT tools, in order to evaluate their use and formulate recommendations.

## List of Figures

Figure 1: issues at stake / topics to address within the whole system development lifecycle ...	10
Figure 2: architecture of the video-surveillance mock-up .....	21
Figure 3: Automatic deletion of data after a defined retention period .....	22
Figure 4: Interface binding and segmentation .....	24
Figure 5: Access logging.....	25
Figure 6: Data storage statistics .....	25
Figure 7: Video extraction .....	26
Figure 8: Standalone tool to check integrity of extracted video files .....	26
Figure 9: Connected Vision module with core task (algorithm) and self-description of the interfaces .....	28
Figure 10: internal and external interfaces of a Connected Vision module.....	28
Figure 11: communication with multiple sources and consumers .....	29
Figure 12: chain of Connected Vision module with secured communication .....	29
Figure 13: reuse Connected Vision module for different analytic tasks .....	30
Figure 14 PEAC in the overall system architecture .....	31
Figure 15 PEAC SQL data model .....	33
Figure 16 Conceptual view of relation of PEAC and SALT framework .....	34
Figure 17 PEAC technical implementation view.....	35
Figure 18: Typical process steps and stakeholders in the use of the SALTmethodology.....	37
Figure 19. Usage of SALT tools for the system designer .....	40
Figure 20 timeline of motion in surveillance video (marked blocks indicates the timeslots where motion was detected).....	42
Figure 21 snapshots of detected motion in videos (sample images are taken from iLIDS video footage) .....	43
Figure 22 Activity diagram of the video analytics system use case .....	44
Figure 23 A record of warrant in PEAC database .....	44
Figure 24 An example of the edit interface for permission in PEAC .....	45
Figure 25 User interface for choosing cameras from a map.....	46
Figure 26 CCTV camera and typical image produced in a transportation infrastructure .....	48
Figure 27: typical video operation room and video operators positions.....	49
Figure 28: Lifecycle of SALT compliant systems .....	51
Figure 29 location of the NVR log and audit tools within the system architecture.....	54

## Abbreviations and Definitions

Abbreviation	Definition
API	Application programmable Interface
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
RTSP	Real Time Streaming Protocol
SALT	Socio-ethicAl, Legal, Technical
SGDSN	Secrétariat General de la Défense et Sécurité Nationale
SPOF	Single Point Of Failure
VAS	Video Analytics System
VCA	Video Contents Analysis
VLAN	Virtual LAN
VMS	Video-Management System
WAN	Wide Area Network
WP	Work Package

WP29	Article 29 data Protection Working Party
------	--



# 1 Introduction

This deliverable is produced in the frame of the Work-Package 5 of the PARIS project, entitled “using SALT for video-surveillance data lifecycle management”, and is related to the following tasks of this WP:

- Task 4: using the framework management tool,
- Task 5: SALT compliant use-case development.

It comes on the aftermath and in coherence with the previous deliverables of the WP5, and especially the D5.2 “Video-Surveillance Lifecycle Management Use Case SALT compliant Framework”. The D5.2 has been dedicated to the explanation of how the SALT tools and the SALT process are applied to the video-surveillance use-case. The D5.2 also features consistent and extensive contents and information to be fed in the SALT repository to handle this use case. These contents have been specified in the form of SALT references, in coherence with the WP2, WP3 and WP4 of the project.

In order to avoid overloading of this document, the SALT references dedicated to the video-surveillance use-case have been extensively shifted within a dedicated document entitled “SALT references for the video-surveillance use-case”; also, these references have been completed with new information and formatted according to the latest templates discussed and agreed within the project.

In addition to the information related to the references, which is available in the abovementioned document, information about complementary SALT contents is provided in the current document: a PIA from a previous FP7 project (ADVISE) related to a system very close to the WP5 one is reused to build a SALT questionnaire; the foundations for a video-surveillance taxonomy are proposed.

In a second part, details about the implementation of privacy-enhancing features in the Network Video Recorder (Thales) and in the Video Archive Search (AIT) are provided.

These enhancements have been defined carefully with respect to the recommendations arising from parallel studies about privacy and video-surveillance; this enables to guarantee that the developments performed also demonstrate a backward coherence with the outputs of the SALT tools (questionnaire and references).

This coherence is demonstrated in the last part of the document, which aims at providing a storytelling canvas from the adoption of the SALT user perspective.

This D5.3 document is also built keeping in mind the forthcoming D5.4 deliverable entitled “Video Surveillance Lifecycle Management Use Case Evaluation”, devoted to the evaluation of the SALT tools and processes based on the video-surveillance use-case based experiences.

## 2 SALT Framework specialized for Video-surveillance

The goal of this deliverable is mainly to provide exemplification for the generic SALT management concepts and tools provided in the following Work-packages of the project:

- WP2 for the concepts of SALT frameworks,
- WP3 for the SALT Framework management tools,
- WP4 for the SAT compliant processes.

SALT has been designed in the aforementioned work-packages to address surveillance systems of any kind (one can argue that the design being very generic, it may cover even wider areas of knowledge).

The examples taken to demonstrate and test the SALT tools and methodology are related to video-surveillance systems in the WP5, and to biometrics in the WP6. The use case in the WP5 is more precisely related to video-surveillance systems in public spaces, and to the use of recording technologies and automatic video contents analysis; this configuration might appear as one of the potentially most infringing for data subject's privacy. Last but not least, the legislation being variable with respect to the country of application, the use case is located in France (remembering it remains a fictitious case, no concrete system is directly or indirectly addressed).

The SALT tools and processes might apply, depending on the case and on the intentions of the stakeholders dealing with this case, at any stage of the process related to the surveillance system (from the concept stage to the operation and maintenance of the system, even extended to the system retirement, though this might appear as of lesser importance and extent). The main issues at each stage of the project are briefly explained on the figure below.

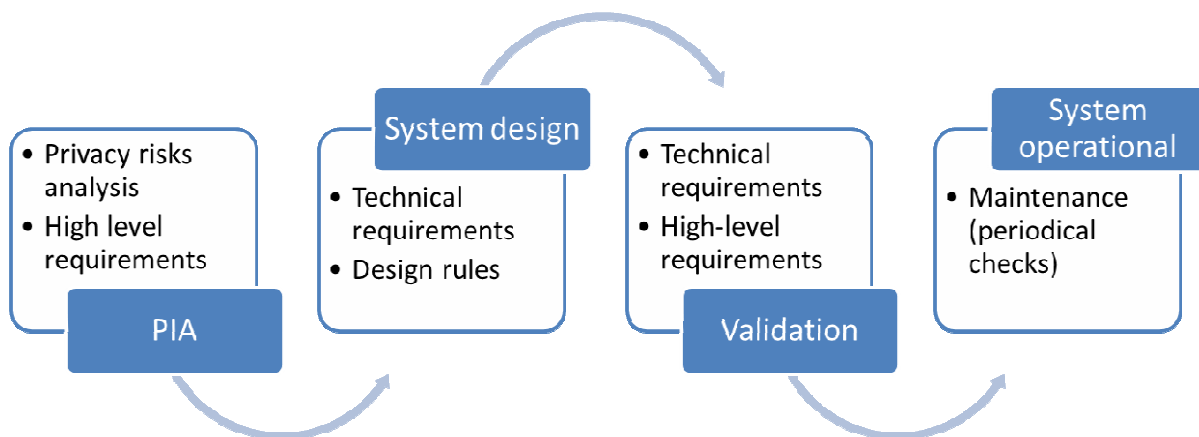


Figure 1: issues at stake / topics to address within the whole system development lifecycle

This presentation is generic (not customized for a given type of surveillance system). One may note that the PIA (Privacy Impact Assessment) is mainly seen in this process at the very upstream phase (this will be commented and a bit opened further, in the chapter dedicated to SALT questionnaires).

The PARIS goal is to provide coherent and completed tooling and methodology to address privacy and accountability alongside the whole engineering chain of a surveillance system; this encompasses the PIA, as just discussed, but also provides Privacy By Design (PbD) concrete implementation possibilities, and possible links to PET (Privacy Enhancing Technologies). The tooling process is also taking into account additional needs for the concrete exploitation of the SALT tools.

The specialization for the Video-surveillance use-case could arise mainly at 2 levels: specialization of the SALT tools, and specialization of the SALT contents; nevertheless, the tools being generic and common to all surveillance systems, it is here only the filing of the SALT with relevant information which makes the specialization. The SALT data related to the video-surveillance use-case that will be populated in the SALT Repository are of three types, all possibly related to any type of contents categories (Technical, Legal, Socio-Ethical). These three types of contents are:

- SALT references, which contain structured and tagged information, and also in some cases precise constraints on the system,
- SALT taxonomies, which contains explanation for words and concepts that fall in the domain “common knowledge”,
- SALT questionnaires, that enable to guide stakeholders to address mandatory points, and that also enable to raise awareness on some points, especially regarding non-purely technical points, such as privacy.

Most of these contents can be used at any stage of the system lifecycle. Nevertheless, references might mainly be used within upstream concept phase and design phases, whereas questionnaires are predominantly of use within the intention phase and within the operation & maintenance phase.

The goal of the following parts of this document is to explain how the video-surveillance related data is gathered and fed in the SALT framework in order to address the use-case.

## **2.1 SALT contents: Questionnaires**

The ADVISE project (“Advanced Video Surveillance archives search Engine for security applications”) focuses on a video-archive search system that is very close to the one developed in the WP5 of the PARIS project. The approach of ADVISE is nevertheless a bit different from the one of the PARIS project as it goes deeper within all facets of such a system: from technical possibilities and enhancements of processing of videos, operational usages, but also ethical and privacy-related dimensions.

From this point of view, the approach to the latter is reusable within the PARIS project, in the frame of the WP5 use-case. The ADVISE deliverable D2.3 “identification of practices and procedures of compliance for the use of video-surveillance archives” is the deliverable that embeds the contents on these points.

Regarding privacy and ethics, the same main concepts as the ones underlined in the WP2, WP3 and WP4 are cited as theoretical grounds in the ADVISE deliverable; these are PIA (Privacy Impact Assessment), PbD (Privacy by Design), and PET (Privacy Enhancing Technologies). This commonality in the approaches between both projects is an interesting confirmation of the PARIS methodology: the ADVISE project, dedicated to the analysis of a very specific system (video surveillance archive search), has provided results completely in-line with the generic principles proposed in the PARIS project.

The conclusion of this ADVISE deliverable about the theoretical analysis of the tools for privacy and ethical analysis and enhancements is that a PIA might be the most efficient approach with widest scope “We argue that PIA comprises both concepts of privacy by design and of privacy by default as well as provides a framework for application of PETs”. In the report, the notion of Ethical impact assessment, close to the one of PIA is also cited.

The PIA proposed in ADVISE is reproduced in the first annex of the current document. It consists of a questionnaire, with explanations for most of the steps. This questionnaire addresses mainly the following points about video-surveillance system components:

- technical description,
- Description of information flow, including personal data (“personal data mean any information relating to an identified or identifiable natural person”),
- Questions related to the recording itself,
- Risks identification,
- Risk assessment,
- Recommendations for the design of the component/system.

This questionnaire is a very good candidate for being integrated in the SALT repository for the WP5 video-surveillance use case; it has been included within the SALT framework, using the SALT tools. As a PIA, it might be used in any stage of the system lifecycle; nevertheless it seems especially suitable for the concept stage (some parts about the technical description of the system being then optional), design phase, and for the operation & maintenance phase, where it is more likely to be used for the assessment of an existing system (from privacy an ethics points of views).

## **2.2 SALT contents: References**

The second type of information that is hosted within the SALT framework for the WP5 video-surveillance use case is made of references. These references are stored in a flexible repository hosting contents of any kind related to the topic: it can be of legal, technical, ethical sort, and even in the middle (mix of domains in the same SALT reference).

In addition to host formatted information of use in the application domain targeted, the SALT references provide two types of central added values:

- They attach description and classification fields to the contents, both at the reference level and at the “concern” level: concerns are atomic components of the references. The classifications are performed on several axis, including but not limited to: geographical

domain of application, type of contents, external reference, classification of contents and keywords. This enable users to browse and to retrieve the relevant information for their use case with maximum performance and flexibility,

- They embed restrictive and unilateral rules that can be verified on the system designed. These rules are of OCL type (Object Constraint Language), they apply on the technical model of the system (UML, Unified Modeling Language); this technical representation being closely used to describe (and even to generate) the system itself, the verification applies indirectly to the live system. The writing of these rules remains optional (because a validation of guidelines can be performed by other means; also because some concerns are too wide and/or ambiguous to be formally described by OCL rules).

The template for the SALT references (common to the whole PARIS project, and used also in the WP6 dedicated to the biometrics use-case) is given below. The references used for the WP5 use-case are reported in Section 8. A list of these references is nevertheless provided below.

### 2.2.1 References template

The reference template given below is both used in the description document of the WP5 references and within the SALT repository as the structure of the reference data: this is an exact image of the way the references are stored and retrieved using the SALT tools.

Field	Type	Description
<b>Reference name</b>	Mandatory	Name that serves to identify the reference, that should be as descriptive as possible. In case the references correspond to a law, an article, a report or any other official document, the name should be the title of that document.  In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen.  Example:  <i>Organic Law 15/1999 on the Protection of Personal Data - Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal</i>
<b>Original language</b>	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
<b>Abstract</b>	Optional	Brief summary of the contents of the reference (~ 100 words maximum) In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields).
<b>Link to source</b>	Optional	Link to the source of information in the original language
<b>Link to translation</b>	Optional	Link to the source of information translated to English
<b>Official translation</b>	Optional	[Yes, No] This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies).
<b>System type</b>	Mandatory	The system type to which the reference applies.  <i>Possible values: Video surveillance systems / Biometric systems / All systems</i>

<b>Geographical Scope</b>	Mandatory	A first layer of context information, which will define the territorial scope of application. The SALT Framework Tool for the creation of references will provide a drop down list containing a set of predefined countries (by now, all the European countries and also the option "European Union" to cover all them). There is also the option "Any" for the cases where this information is not relevant for the reference (e.g. technical information).
<b>Context</b>	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference ( <i>e.g. specific cases/conditions where the reference is applicable</i> ).
<b>Version</b>	Mandatory	Version of the reference in the format vA.B. By default this field has the value: v0.1
<b>Keywords</b>	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the reference
<b>Creator</b>	Automatic	Person responsible for the creation of the reference in the SALT Repository ( <i>automatically filled by the SF Tool</i> )
<b>Last update</b>	Automatic	Date and time of the last reference update ( <i>automatically filled by the SF Tool</i> )
<i>List of concerns (privacy and accountability related concerns for surveillance systems)</i>		
<b>Concern ID</b>	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
<b>Name</b>	Mandatory	Title for the concern, which should give a brief idea of the contents or aspects covered by the concern. The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A text would probably include more than one concern. In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: Duty to inform - Deber de informar
<b>Additional information</b>	Optional	Extra information that helps readers find the concern in the source text.
<b>Description</b>	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc.
<b>Category</b>	Mandatory	Category of the concern, that can be one or several among this options: <i>Legal, Socio-Ethical, Technical</i> .
<b>SALT Topics</b>	Optional	SALT legal topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks. The list of defined SALT legal topics, and its mapping with the privacy principles indicated in ISO Standard 29100, is available in Section 9.
<b>Stage</b>	Optional	Stage or stages of the SALT Process in which this concern applies. These are the stages defined and their goals: <ul style="list-style-type: none"> <li>• <b>concept</b> (intention): selection of the most suitable solution to solve the stakeholder's problem;</li> <li>• <b>design</b>: elaboration of the system design according to the different requirements;</li> <li>• <b>development</b>: implementation of the system based on the defined</li> </ul>

		specification; <ul style="list-style-type: none"> <li>• <b>deployment</b>: set up the system in the stakeholder's environment;</li> <li>• <b>operation &amp; maintenance</b>: use the system and ensure its correct functioning to satisfy stakeholder's needs;</li> <li>• <b>retirement</b>: shut down the system in a controlled manner.</li> </ul>
<b>Keywords</b>	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern.
<b>Guidelines</b>	Optional	Any guidance on how to include the concern in the development of the system. This could be a concrete artifact or solution, a strategy or procedure, or just any tip about how to take this concern into consideration.
<b>OCL Rules</b>	Optional	One or several OCL rules that allow to verify that the system addresses the concern. The OCL expert needs to fully understand the meaning of the privacy/accountability concern for which the OCL rules are created. These rules will be used for the automated (or human assisted) validation of the concern it relates to, once its corresponding solution provided by the SALT reference has been implemented in the system design.  OCL rules are only available for the design stage (in parallel with the UML profile).

## 2.2.2 References list

The SALT references related to the WP5 use-case are in Section 8.

These references are there mainly for the sake of example; they raise the capability to perform an end-to-end demonstration of the use of the SALT tools and processes through the video-surveillance use-case. They have been carefully collected for the three lines of knowledge of interest to the SALT framework: the legal theme, the socio-ethical theme, and the technical theme; this list of references might not be fully exhaustive however.

As explained further in this document, this set of references is a base of knowledge that is intended to be browsed using the SALT framework tools in order to perform a selection of those of interest to a given project. The references will be integrated within the SALT repository in order to demonstrate these steps (browsing and selection).

This section documents the list of references collected for the video-surveillance use-case.

### 2.2.2.1 Legal references

References description. Fields	References descriptions
<b>Reference name</b>	<b>Belgium law on video-surveillance 2007 – Loi réglant l’installation et l’utilisation de caméras de surveillance</b>
<b>System type</b>	video-surveillance systems

<b>Geographical scope</b>	Belgium
<b>Reference name</b>	<b>Title V “Videoprotection” of the French Homeland security Code – Code de la sécurité intérieure, Titre V “Videoprotection”</b>
<b>System type</b>	video-surveillance systems
<b>Geographical scope</b>	France
<b>Reference name</b>	<b>French ministerial Decree of 3 August 2007 on technical requirements of videosurveillance systems – Arrêté du 3 août 2007 portant definition des norms techniques des systèmes de vidéosurveillance</b>
<b>System type</b>	video-surveillance systems
<b>Geographical scope</b>	France
<b>Reference name</b>	<b>Code of Criminal Procedure – Code de procédure pénale</b>
<b>System type</b>	All systems
<b>Geographical scope</b>	France
<b>Reference name</b>	<b>Act n°78-17 of 6 January 1978 on Information Technology, Data Files ad Civil Liberties – Loi du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés</b>
<b>System type</b>	All systems
<b>Geographical scope</b>	France
<b>Reference name</b>	<b>EU Law Enforcement Data Protection Directive Proposal (pending legislative act – not approved)</b>
<b>System type</b>	All systems
<b>Geographical scope</b>	European Union
<b>Reference name</b>	<b>EU data Protection Regulation Proposal (not approved yet)</b>
<b>System type</b>	All surveillance systems
<b>Geographical scope</b>	EU
<b>Reference name</b>	<b>Criminal Procedure Code (Strafprozeßordnung, StPO) on Seizure, Interception of Telecommunications, Computer-assisted Search, Use of Technical Devices, Use of Undercover Investigators and Search</b>
<b>System type</b>	Video-surveillance systems
<b>Geographical scope</b>	Austria

### 2.2.2.2 Technical references

<b>References description. Fields</b>	<b>References descriptions</b>	<b>Technical descriptions</b>	<b>Privacy risks</b>	<b>PET</b>
<b>Reference name</b>	CNIL Security Guide			
<b>System type</b>	All			
<b>Geographical</b>	France	*	**	**



<b>scope</b>				
<b>Reference name</b>	<b>Denial of service risk IT attack on camera</b>			
<b>System type</b>	All video-surveillance systems	**	***	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Encryption and signature of video data: principles and benefits</b>			
<b>System type</b>	All video-surveillance systems	**	*	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Logical access control to video-surveillance systems</b>			
<b>System type</b>	All video-surveillance systems	*	**	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Capabilities of google-glass cameras</b>			
<b>System type</b>	All video-surveillance systems	**	*	*
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Logs and audit tools about operator actions for enhanced accountability</b>			
<b>System type</b>	All surveillance systems	**	*	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Resolution of video images and recognition performances</b>			
<b>System type</b>	All video-surveillance systems	***	***	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Scalability of video analytics</b>			
<b>System type</b>	video-surveillance systems	***		
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Detection quality of video analytics</b>			
<b>System type</b>	video-surveillance systems	***		
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Privacy risks management</b>			
<b>System type</b>	video-surveillance systems	*	**	*
<b>Geographical</b>	Worldwide			

scope				
<b>Reference name</b>	<b>Architecture pattern: access control for video archive search</b>	***	*	**
<b>System type</b>	All video-surveillance systems			
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Interoperability of authentication and identity management</b>	***	*	*
<b>System type</b>	All surveillance systems			
<b>Geographical scope</b>	Worldwide			

### 2.2.2.3 Socio-Ethical references

References description. Fields	References descriptions
<b>Reference name</b>	<b>2008 CNIL study : French people and videosurveillance”</b>
<b>System type</b>	All video-surveillance systems
<b>Geographical scope</b>	Worldwide
<b>Reference name</b>	<b>“Surveillance ethics from the Internet Encyclopedia of Philosophy”</b>
<b>System type</b>	All surveillance systems
<b>Geographical scope</b>	Worldwide
<b>Reference name</b>	<b>“video-surveillance in retail places: ethical perspective ”</b>
<b>System type</b>	All surveillance systems
<b>Geographical scope</b>	Worldwide

## 2.3 SALT contents: Taxonomies

The third and last type of contents stored in the SALT repository using the SALT tools are the taxonomies. In the frame of the PARIS project use-cases, there will be at least two taxonomies: one dedicated to the video-surveillance systems, and other to the biometrics systems.

Taxonomies are transversal to all the system lifecycle stages and common to the other SALT tools (SALT references and SALT questionnaires); they are supporting capabilities for the information, formation and awareness of the stakeholders wishing to gather and use information from the SALT framework.

They mainly appear as dictionaries, each of which contains definitions of several words of importance in the field of application.

A list of the terms of interest (in the process of building the taxonomy) for the use-case is provided in the subsection below. It lists the terms to be explained (definitions, such as the resolution of an image and the data throughput of an image).

The list below contains the terms that are to be explained within the taxonomy related to video-surveillance in the frame of the WP5 use case. The goal is to provide this for the sake of the example, not to provide an exhaustive list that could be enriched.

<b>word</b>	<b>definition</b>
Aperture	The aperture of a camera is the geometrical surface through which the light enters the lens of the camera; it also refers to the number used to measure this surface. It is expressed as related to the focal of the lens of the camera (such as f/2.8, f/16. The smaller the number is, the bigger the surface is). The aperture has impact on the field of view of the camera, on the amount of light on the camera sensor, and on the sharpness of the image produced.
Autofocus	The autofocus is a capability for a camera to automatically tune to obtain optimal image sharpness on a physical object within the image. This capability is available in most of the modern cameras; it can be performed using several ways, among them, distance measurement to the object, use of a contrast detector.
CCD	The Charged Coupled Device technology is one of the most used semiconductor technologies to build the electronic sensor that produces an image from light within a camera.
CMOS	The Complementary Metal-Oxide-Semiconductor technology is one of the most used semiconductor technologies to build the electronic sensor that produces an image from light within a camera.
Compression	The compression of a video stream is the type of IT format that is used to encode the video stream. Most of the compression formats carry streams that have been computationally altered to strongly lower their size in memory (number of Bytes produced per second); “compression” also often refers to the type of numerical algorithm that is used to “compress” the stream. Most often, the compression is said “destructive” meaning that some information is missing in the produced stream; however the algorithms are optimized to ensure that the degradation in quality is sufficiently low (at least that this degradation is mastered). The typical compression formats that are used are the ISO MJPEG (Moving Joint Photographic Expert Group), MPEG (Moving Picture Expert Group).

Field Of View	The Field of View (FOV) of a camera is the zone of the scene where the image appears sufficiently sharp. It is often defined by the minimum distance of sharpness and the maximum distance of sharpness.
Resolution (camera resolution)	The resolution of an image is the number of lines and the number of columns of pixels within an image produced by a camera. An example current typical resolution is HD-720p, featuring 720 lines and 1280 columns. However, it is sometimes referred to spatial resolution of an image, expressed typically in pixel per inch; this is the equivalent number of pixels that will be imaged on a physical object for a physical distance of 1 inch. This parameter is more complex to handle as this varies with most of the camera parameters, alongside with the distance from the object to the camera.
Sensor (camera sensor)	The sensor of a camera is an electronic component that produces the image from incoming light. It is made of an array of elementary photo-sensors that produce an electrical parameter which magnitude depends on the quantity of light received. The camera sensor is one of the most important components of a camera.
Video Archive Search	Video Archive Search (VAS) refers to technologies that enable to intelligently and/or automatically browse image recordings in order to localize a given event or event pattern (example pattern: a van exiting a car place).
Video Content Analytics	Video Contents Analytics are technologies providing automatic analysis of video streams, live or recorded, in order to detect pre-defined patterns (such as motion, abandoned luggage, face..).

### 3 Refined description of the architecture of the mock-up video-surveillance system

The technical mock-up produced by Thales and AIT for the video-surveillance use-case has been defined in coherence with the analysis performed within the previous WP5 deliverables (mainly D5.1 and D5.2). This analysis enables to guarantee that the developments performed contribute to improve the privacy of data subjects and the accountability of the organizations and persons prescribing, defining, developing and using this type of video-surveillance system. Also of key interest is that the developments and improvements performed enable to bridge with the contents of the SALT framework dedicated to the use case (cf. §36).

This document section provides a reminder regarding the architecture of the system, and details about the capabilities that have been implemented to foster and enhance the privacy and accountability performance of the system.

#### 3.1 General architecture of the system

The figure below depicts the global architecture of the video-surveillance mockup, with the main interaction points with the uses, and the identification of the places where data are recorded.

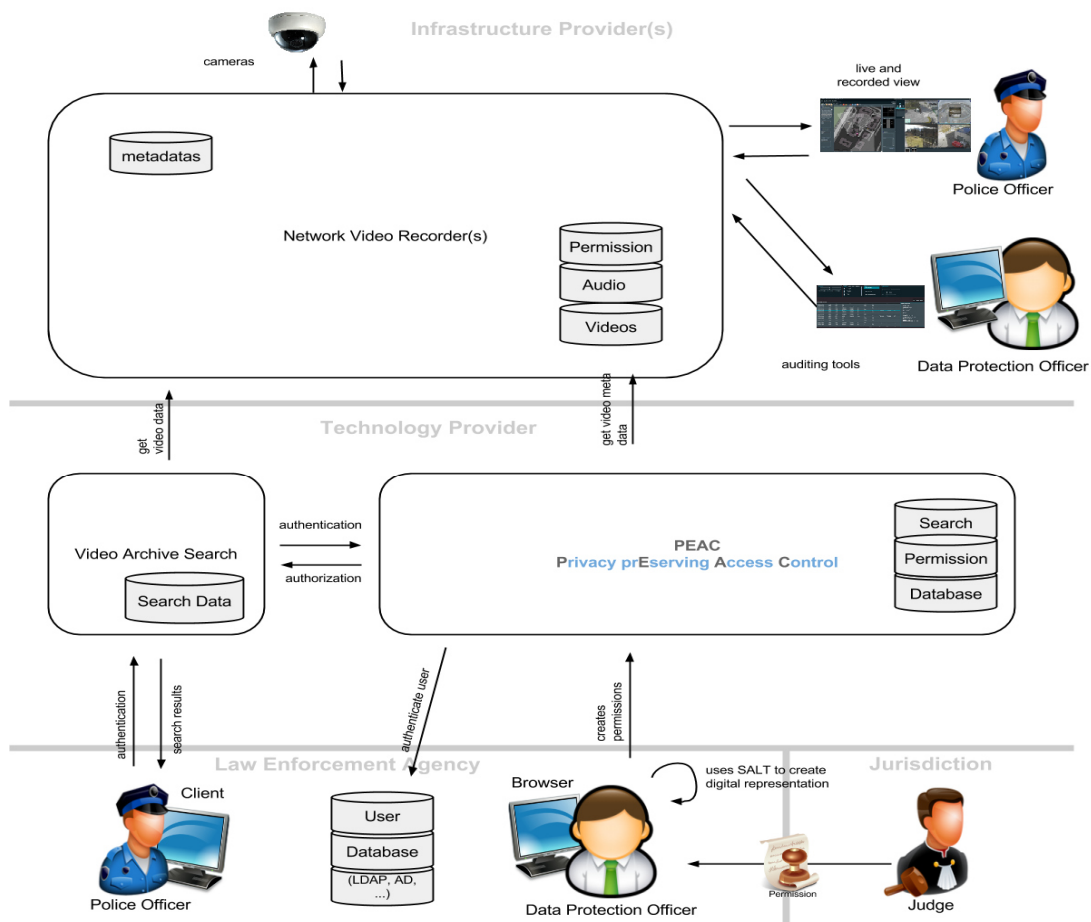


Figure 2: architecture of the video-surveillance mock-up

## 3.2 Detailed architecture of the NVR and privacy-enhancing components and developments

### 3.2.1 Presentation of the Thales NVR

The Network Video Recorder is a key component of a video surveillance system. Its role is to record the video streams coming from configured video sources. The NVR is therefore a very sensitive sub-system and precautions need to be taken to preserve the privacy of citizens.

These precautions include:

- Managing the life cycle of recorded videos, ensuring that local regulations are respected
- Authenticating users accessing the different functionalities of the NVR
- Logging access to sensitive features and resources
- Ensure confidentiality and integrity of the data stored and extracted

The Thales NVR presents multiple features:

- Recording video/audio streams
- Managing storage, automatically deleting old data according to configuration (cf. Fig. 1)
- Locking important recorded data, extending their lifespan in the system according to configuration
- Indexing recorded data
- Streaming recorded video/audio streams
- Exporting video/audio clips

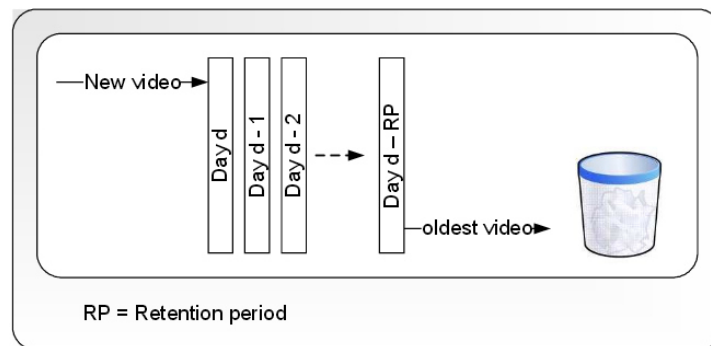


Figure 3: Automatic deletion of data after a defined retention period

Many of these functionalities are accessed either via authenticated RTSP (for media streaming) or via an HTTP API.

As part of the PARIS project, enhancements to the Thales NVR have been identified and developed:

- Improvements to the authentication methods for the HTTP API as well as the RTSP streaming protocol, allowing for better filtering of access to privacy-sensitive data
- Usage of strong cryptographic ciphers to ensure data confidentiality when using the HTTP API

- Stronger methods for storing passwords, preventing attacks that would give malicious users unauthorized access to privacy-sensitive data
- Network interface binding, allowing a strong physical or logical separation between networks used for managing the NVR and recording/streaming videos
- Automatic logging of user actions, such as HTTP API accesses and RTSP streaming of recorded videos
- User-friendly method for retrieving the age of the data stored, to ensure that the defined data lifecycle is respected
- Cryptographically signed video extracts, ensuring that the integrity of the video has not been violated

These developments are detailed hereafter.

## 3.2.2 Enhancements and developments

### 3.2.2.1 Authentication

#### 3.2.2.1.1 HTTP(S) API

The NVR exposes an HTTP API that allows the user to manage its different components (extraction of videos, locking of tracks...). The built-in HTTP server supports both HTTP and HTTPS protocols, the latter being privileged.

HTTPS is a secure protocol that provides authentication and end-to-end encryption of data. Using HTTPS while authenticating users and accessing sensitive data prevents attacks, eavesdropping and tampering regarding the contents of the communication.

If configured, authentication is made mandatory for sensitive URLs, the user having to login prior to using the API. Different user roles are configurable, to allow for fine-grained configuration of permissions.

As part of the PARIS developments, the protocols and cipher suites used for HTTPS connections have been restricted to ensure the best protection against known attacks (e.g. SSL v2/v3, EXPORT suites are disabled...).

Optionally, client-side authentication can also be configured. With this configuration, both the server and the client identities are verified using certificates and strong cryptography.

#### 3.2.2.1.2 Password storage

Passwords used for authentication are stored in the NVR's main configuration file. Within the context of the PARIS project, enhancements have been added to the way these passwords are stored.

Algorithms that are used to store passwords securely rely on hashing functions, *salting* and a (configurable) high number of iterations, with the purpose of being *as slow as possible* without impacting user experience. Using a slow function drastically increases the time needed to find the password using *brute force*, i.e. trying every possible combination until the password is found. Moreover, the configurable nature of these algorithms is meant to adapt the *slowness* if needed, for instance when more powerful machines are available.

As of today, the password management code only supports PBKDF2 storage and plaintext storage (for compatibility purposes) but other algorithms can be added, notably to keep track of the attackers growing computing power of *breaking* algorithms. When a better algorithm is implemented, the NVR will automatically change the storage of the users' passwords on their

next login to use the best algorithm. This allows the NVR to upgrade its storage method transparently and to always use the safest method available.

### 3.2.2.1.3 RTSP authentication

The NVR is able to stream previously recorded videos using the RTSP protocol. Authentication is configurable in the main configuration file and, if enabled, restricts access to video streams only to configured users.

The streamer supports Basic Authentication as well as Digest Authentication.

While Basic Authentication uses no cryptography whatsoever and transmits username and password in plaintext, Digest Authentication provides a method for authenticating using cryptographic hashes without having to transmit the password in plaintext.

### 3.2.2.2 Network interfaces binding

To add flexibility to the way the NVR is integrated in systems, the network interfaces used for the HTTP Server as well as the RTSP Server can now be specified.

This new feature, developed within the context of the PARIS project, can be used in different scenarios:

- By using a VPN and binding a server to the virtual interface created by the VPN, one can easily add another layer of security to the HTTP API or the RTSP server.
- The functionalities can be segmented between different networks, either physical (different network cards) or logical (VPN), preventing unauthorized access to video streams. Such a separation is illustrated in Fig. 2.

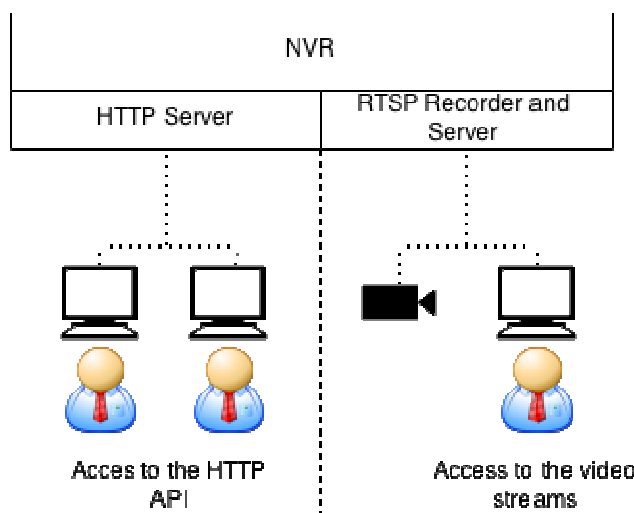


Figure 4: Interface binding and segmentation

### 3.2.2.3 Logging user events

In addition to video streams, the Thales NVR can record metadata streams formatted as XML. This feature is leveraged to log user access to the NVR resources. A dedicated *metadata track* records user login / logout, accesses to sensitive HTTP API endpoints as well as RTSP streaming actions.



This *metadata track* can be extracted from the NVR the same way as video tracks, and can also be consulted on a dedicated HTTP page (cf. Figure 5: Access logging).

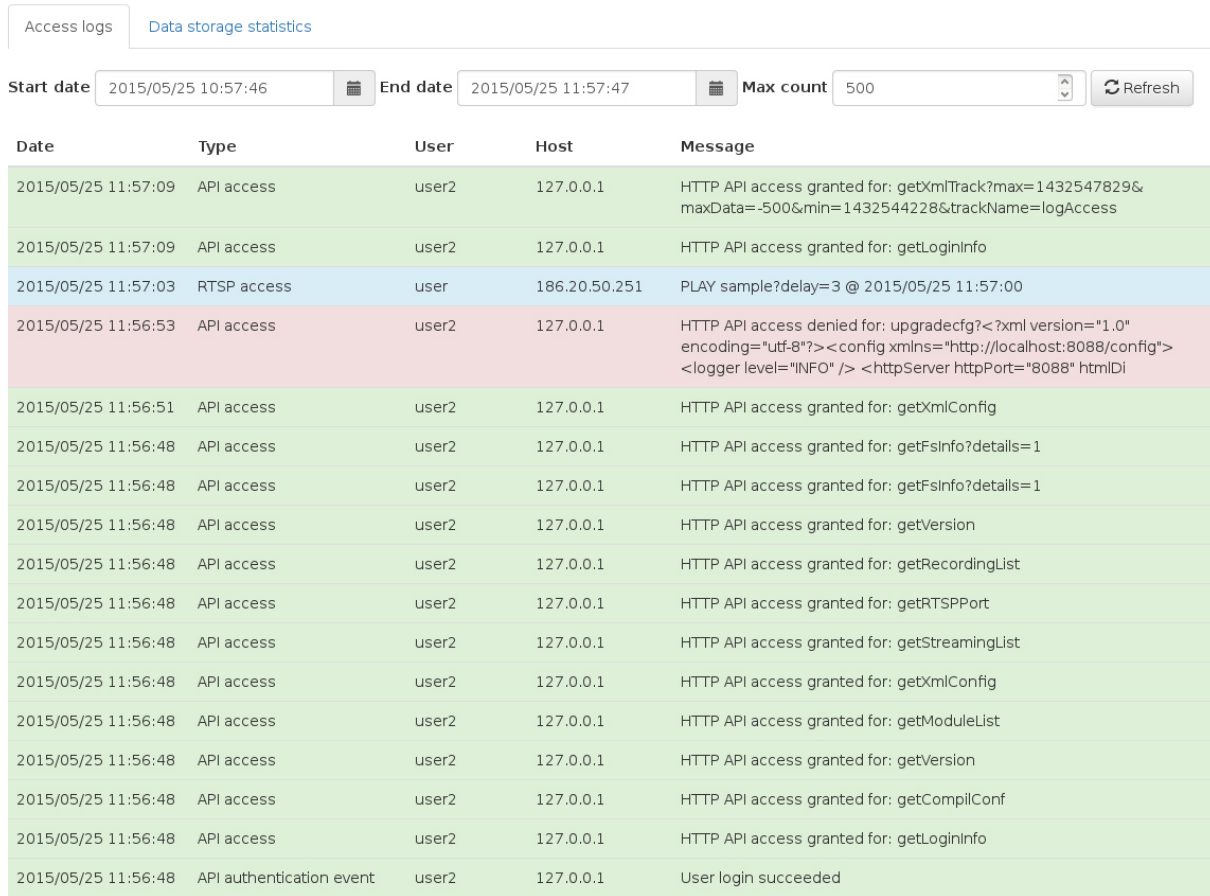


Figure 5: Access logging

### 3.2.2.4 Data storage statistics

A dedicated web page has been added to the PARIS developments to allow end-users to easily get information about the age of stored data (cf. Figure 6: Data storage statistics). This new feature can be leveraged to ensure that privacy-sensitive data is indeed not kept indefinitely. Moreover and as stated before, the NVR can be finely configured to automatically delete data after a certain amount of time.

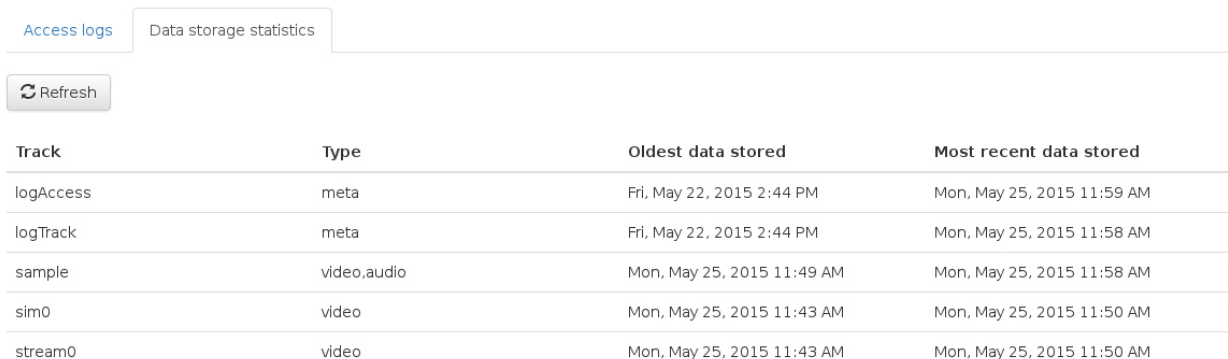


Figure 6: Data storage statistics

### 3.2.2.5 Signed video extracts

The Thales NVR can extract recorded video as video files (e.g. as an .avi or .mkv file) by calling a dedicated API method. An HTTP page has also been added as part of the PARIS developments to easily generate and download video files (cf. Figure below).

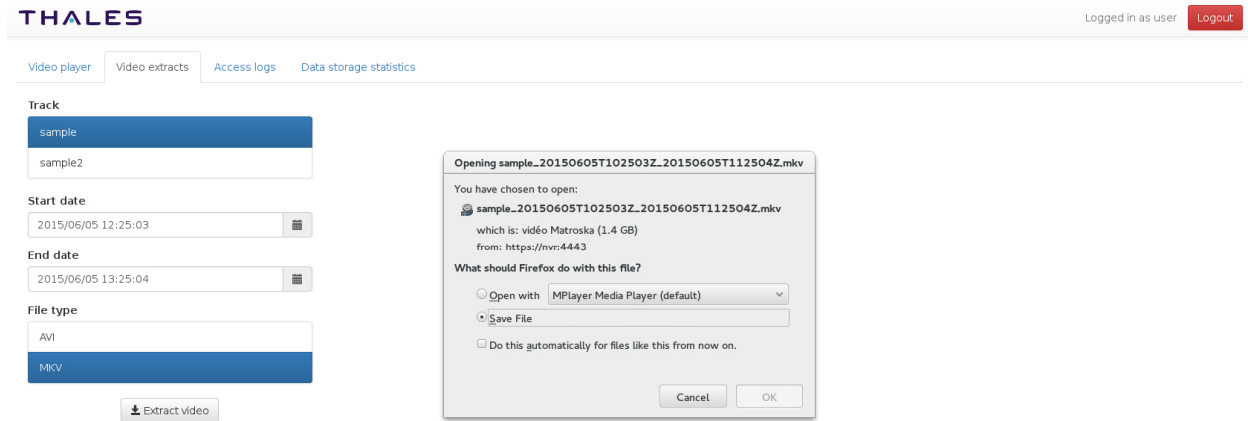


Figure 7: Video extraction

Within the context of the PARIS project, the video extraction module has been extended to provide cryptographic signatures that can be checked to ensure the integrity of the extracted video file. By specifying in the NVR's configuration the desired type of signature and the private key to use for signing, a digital signature (using for instance SHA256-RSA) is computed and appended to the video file.

A standalone tool has also been developed to easily verify the integrity of the resulting video file (cf. below).

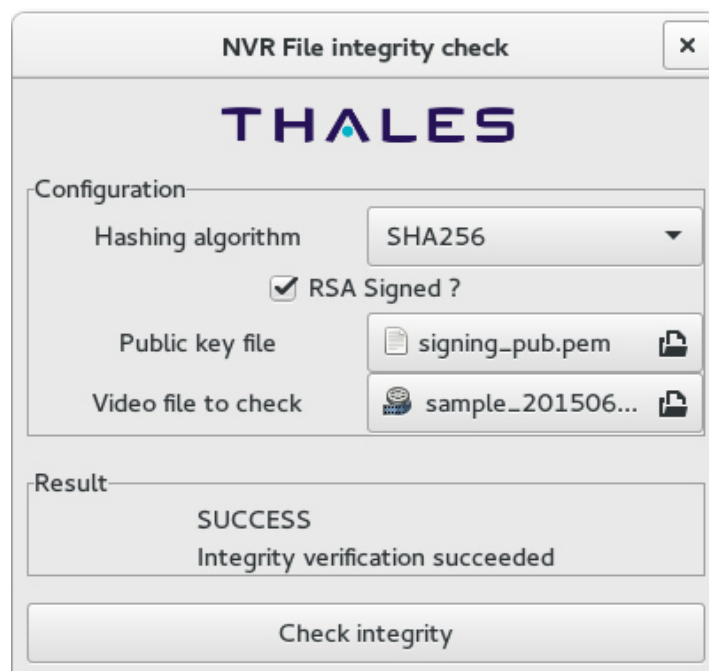


Figure 8: Standalone tool to check integrity of extracted video files

This feature can provide insurance that an extracted video file has in no way been compromised on its path between the NVR and the end user's computer.

### **3.2.3 Ideas for further improvements**

To improve confidentiality and integrity of data streamed from the NVR, the SRTP protocol could be implemented. It provides encryption, message authentication and integrity as well as replay protection to RTP streamed data. Unfortunately, SRTP support is not widely developed amongst popular video players.

The NVR can also be modified to use Hardware Security Modules (HSM), using the PKCS#11 standard. This would allow for a much stronger security, because all of the cryptographic computing would happen in the HSM without divulging the private cryptographic material to the software.

## ***3.3 Detailed architecture of the VAS and privacy-enhancing components and developments***

### **3.3.1 Video Analytics System**

The video analytics system used to demonstrate this use-case is implemented as a modular, micro-service architecture. It is based on the Connected Vision framework that offers a flexible way to implement and combine various computer vision algorithms in a distributed manner, and provides a comprehensive Software Development Kit (SDK) for rapid application development.

Connected Vision offers a flexible basis to solve complex computer vision tasks. The common approach to solving such tasks is to split them into smaller and better manageable parts. These small parts of a complex task are represented by basic building blocks of the Connected Vision framework – denoted as modules. To solve a complex computer vision task, two or more modules are combined to build a module chain.

Each module implements a self-contained core task (e.g. an object tracker, a person detector, filtering) and follows a self-descriptive approach, which is provided through a human- and machine-readable interface using JavaScript Object Notation (JSON). In this way, each module offers information about its inputs, outputs and configuration (settings) to the outside world, called self-description (see Figure 9). The self-description is the starting point of the module design and is the first artefact that needs to be written. This is the input for the generator supplied by the Connected Vision SDK to create the module skeleton, interface classes and the storage (e.g. data-definition-language in case of a database).

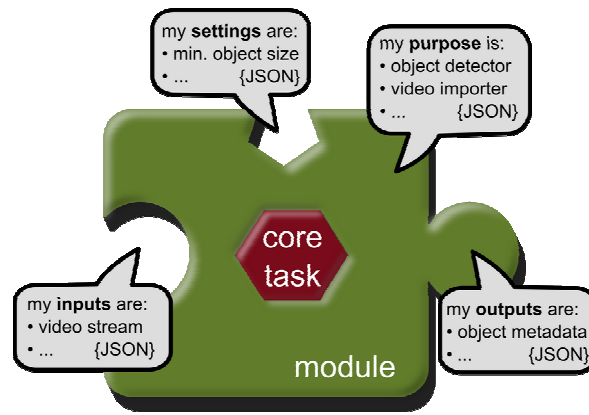


Figure 9: Connected Vision module with core task (algorithm) and self-description of the interfaces

Internally, the access to input data, configuration and also the access to the module storage, are realized through a uniform abstraction layer (see Figure 10). Having a uniform storage layer ensures that module results – binary as well as metadata – can be kept in arbitrary types of storage without affecting the actual implementation of modules' core tasks. Also, having a uniform communication layer / interface ensures that modules can be connected together without the need of any adapters.

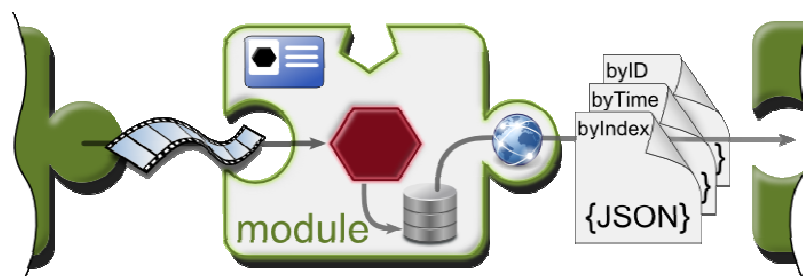
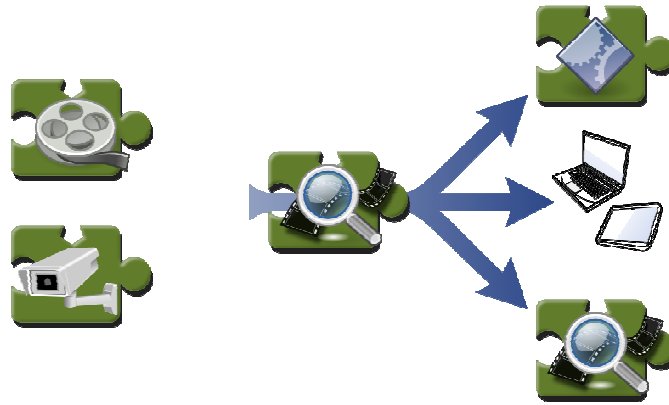


Figure 10: internal and external interfaces of a Connected Vision module

Another advantage of this architecture style is that security measure can be applied directly to the storage and communication layer without interfering with the core task of a module. This means, privacy protection actions can be implemented to a system with existing modules by injecting them on the common interface layers (see also Figure 12).

Technically, each Connected Vision module is an autonomous micro-service that communicates via a Representational State Transfer (REST) interface, collects data from multiple sources (e.g. real-world physical sensors or other modules' outputs), processes the data according to its configuration, stores the results for later retrieval and provides them to multiple consumers (see Figure 11). The communication protocol is designed to support live (e.g. network camera) as well as archived data (e.g. video file) to be processed.



*Figure 11: communication with multiple sources and consumers*

The module autonomy is especially reflected in the configuration of module chains that compose the solution of a complex computer vision task (Figure 12), as each module is capable of not only taking its own configuration but also of passing on relevant configurations to its predecessors. Consequently, a higher-level instance that manages chains of modules and their configuration or interconnections between them is not needed.



*Figure 12: chain of Connected Vision module with secured communication*

As the strength of a forensic video analytics system lies in the range of its analytic possibilities. So the modular approach is essential for the various analytics task, requiring different algorithms, which should be processed with the system. It is possible to reuse common modules (e.g. converter or filter modules) and replace only a few modules to provide a module chain for a different search task (see Figure 13).

On the other hand, this rather easy step, of exchanging some modules, to improve the analytic possibilities of the system introduces a privacy concern. Special measures have to be taken into account for modular analytics systems to enforce the requested privacy and security level. A first step is to restrict certain algorithms / modules or module chains to special users and limit them for a dedicated warrant, as it is discussed in section 4.2.2.

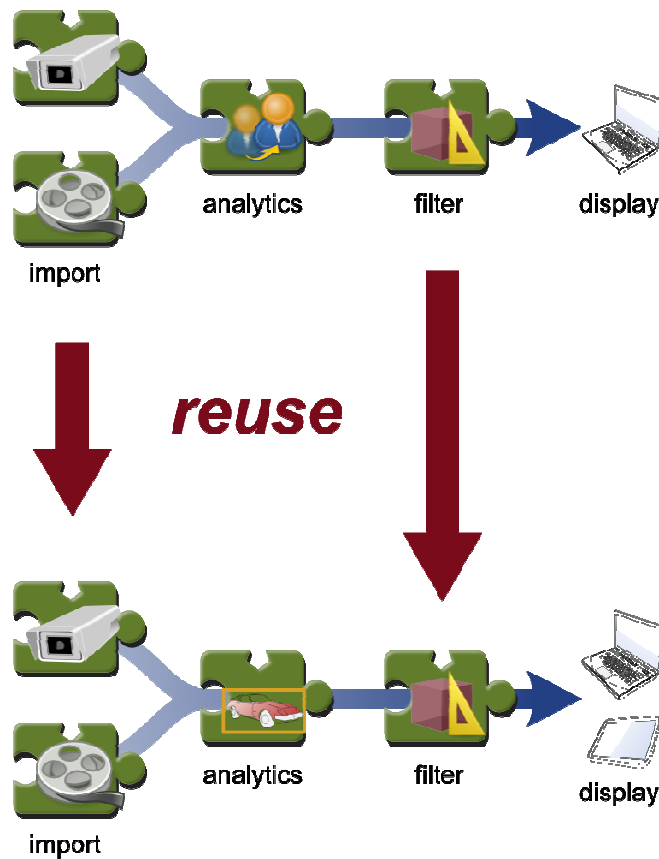


Figure 13: reuse Connected Vision module for different analytic tasks

### 3.3.2 Privacy prEserving Access Control (PEAC)

Privacy prEserving Access Control is an important component of the architecture, which implements the conceptual Policy Enforcement Point (PEP) in the OASIS XACML reference architecture<sup>1</sup> and extends existing information security access control and identity management with privacy policy specification and enforcement functionalities. PEAC is a full featured, standalone, and flexible module for enforcing privacy-preserving access controls. Figure 14 indicates the location of PEAC in the whole system architecture. Although it is used for privacy enhancement for video analytics system in the use case, we envision it can also be used as one of the technical building blocks for all other types of privacy-preserving access control tasks.

<sup>1</sup> OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0, 2013

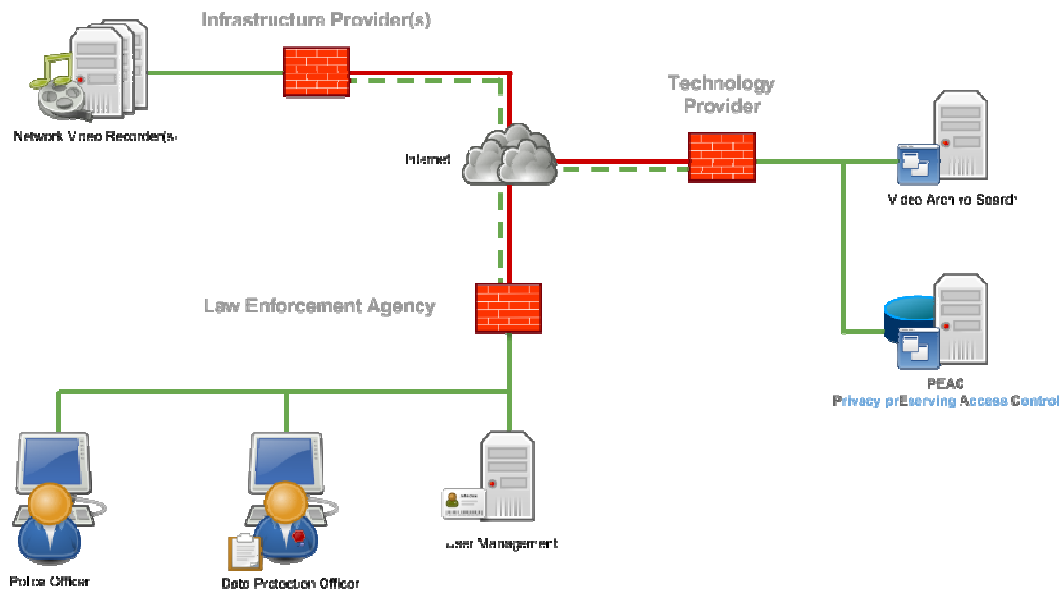


Figure 14 PEAC in the overall system architecture

In addition to general requirements mentioned in this deliverable and D5.1 and D5.2, specific design and implementation requirements related to PEAC include:

- **Widen Adoption.** Although this is a very generic consideration, it is very important as it can drastically increase adoption of such a system. Affected decisions may be: Choice of programming languages, maintainability and integrate-ability.
- **Ease of Use.** The easier the usability, the better chance the user acceptance and avoidance of misconfigurations. The system should be easy to use for technical as well as non-technical people. Requirements and experience necessary to successfully use the system correctly, more specifically, securely, must be kept as low as possible.
- **Interoperability.** Allowing integration into already existing systems, most notably user management, identity management and authentication systems will highly increase adoption into production environments.
- **Dynamic Infrastructure Setup.** Designing the system with modular components will allow deploying organizations to fulfill regulations as well as lowering costs as far as possible at the same time.
- **Applicability in Untrusted Environments.** If parts of the system can be designed to not need critical information or can be secured accordingly, outsourcing can be used to reduce costs even if security demands are high.
- **Supporting Governance Process with Minimum Overhead.** The system should support governance of the entire process through the use of the four-eye principle and double-checking to effectively reduce misuse and abuse. However, sometimes it will increase operational and organizational overhead. Therefore, persons involved in the processes for governance should be kept in a balance between efficiency and privacy oversight.

- **Decentralization.** Keeping the central systems - servers - to a minimum decreases maintenance cost and can increase availability and make the system more independent. This is especially challenging, as the auditing of all actions must be possible according to the requirements.
- **Secure Workflows.** Securing not only communications, but the business logics or workflows cryptographically would be a major security increase, but is also extremely challenging, as security depends more on users, who often don't know what to do, and auditing becomes difficult.

The technical concept in the design aims at fulfilling the above requirements. The design goal of PEAC is to provide an interface for communication with the VAS and an administrative interface for editing access and usage permissions. Administrators can log into PEAC using the web interface. There they are able to create, edit and delete permissions (or can be in the form of a "search warrant" within existing criminal investigation law), cameras, algorithms, infrastructure (video data) providers (in the form of NVRs) and users. Users themselves are not managed by PEAC. It only creates local database entries for needed users for easier data management.

In actual implementation, PEAC uses the "WSO2 Identity Server" as an abstraction layer for user authentication and authorization. The Identity Server provides a unified interface for PEAC and can be connected to authentication and identity management (AIM) technologies such as 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.

Information security models and mechanisms are extended for privacy enhancement. The Security Model describes the used access control models to satisfy the privacy needs. We leverage the following security models:

- **Role Based Access Control.** The right to manage data within PEAC is controlled on a role level. Every user that is assigned to a certain group or role has control over PEAC. Finer granularity is possible, depending on the specification of the access policy. However, we recognize that privacy is more than mere access control, which needs to be addressed in all levels of the system. Access control and its capability should not lull the user into a false sense of privacy and security.
- **Attribute Based Access Control.** The Warrant system is based on Attribute Based Access Control (ABAC). It is also very similar to XACML. Every warrant 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 PEAC is that a request does not contain the action or resource. In this specific use case, the user is authorized by



subject (user) and environment (validity) only. Instead of requesting a specific resource, the user is presented all resources he is allowed to access, grouped by warrants.

Information security mechanisms used for access control include:

- Authentication. When PEAC receives an HTTP Basic *Auth* request, it extracts the username and password and checks if they are valid by asking the Identity Server.
- Authorization. If the Identity Server confirms the credentials, PEAC gets all warrant records where the user is included in the subjects and the current time is a valid environment. PEAC then returns these records to the Video Analytics System.

Records are saved in a SQL database. Its schema is described in Figure 15.

### SQL-UML Hybrid Concept

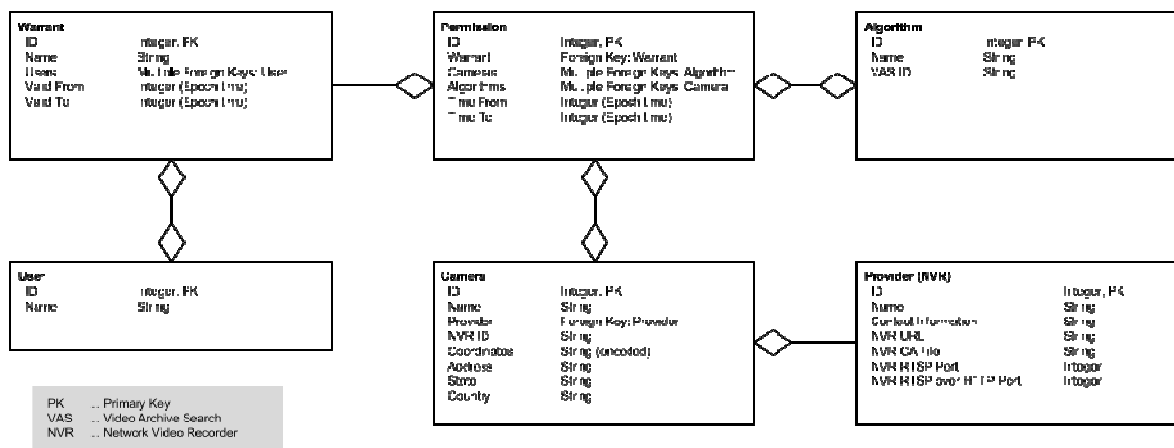


Figure 15 PEAC SQL data model

The Privacy-Preserving Access Policy (PPAP) defines how access should be handled and at the same time represents the requirements for the security model as well as the security mechanism. The specification of the PPAP is given below:

- Only the Data Protection Officer is allowed to edit any data within PEAC. This includes warrants as well as algorithms, cameras and infrastructure providers. Even the permission to edit cameras or algorithms can easily be misused, as the change of a camera may lead to the change of a search warrant, therefore breaking integrity.
- A user is only allowed to access the videos and only within the time frame he is permitted to by the legal system and approved by the Data Protection Officer.
- The combination of videos and algorithms is restricted and may only be used in the way approved by the DPO.
- Users using the Video Analytics System must not be allowed to view the video directly, but only the search output.
- When the Data Protection Officer is creating the digital search warrant record, he is under no circumstances, without exception, to extend permission given by the legal system.

- All actions within PEAC must be documented and saved with integrity.

On the one hand, PEAC can be seen as a technical control that implements the vision, concept, or policy captured by the SALT framework. On the other hand, the design and development of PEAC for WP5 use case also provides technical input in the form of SALT references and feedbacks to SALT conceptual work. The relation of PEAC and the SALT framework is depicted in Figure 16.

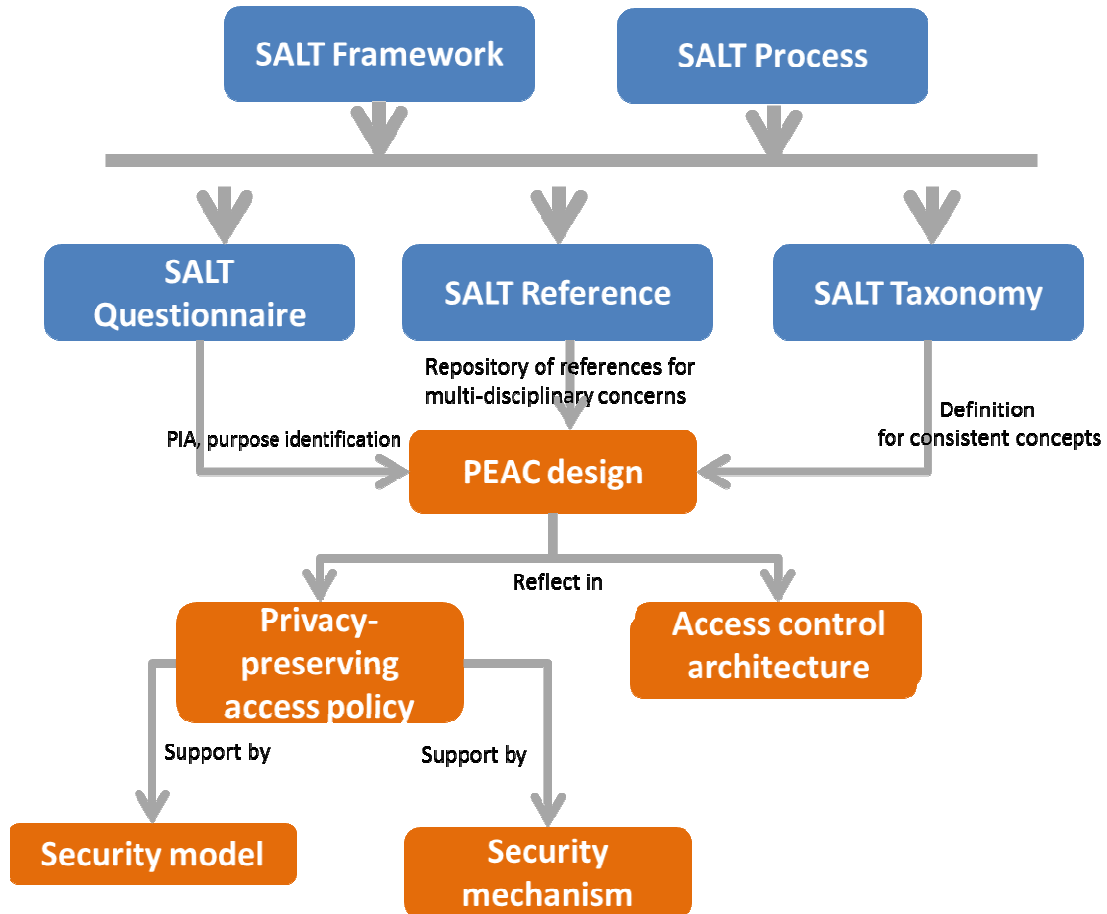


Figure 16 Conceptual view of relation of PEAC and SALT framework

For the proof-of-concept demonstration, PEAC is an under on-going development. The intermediate technical implementation and interface view is given in Figure 17, which reflects the aforementioned concept and design.

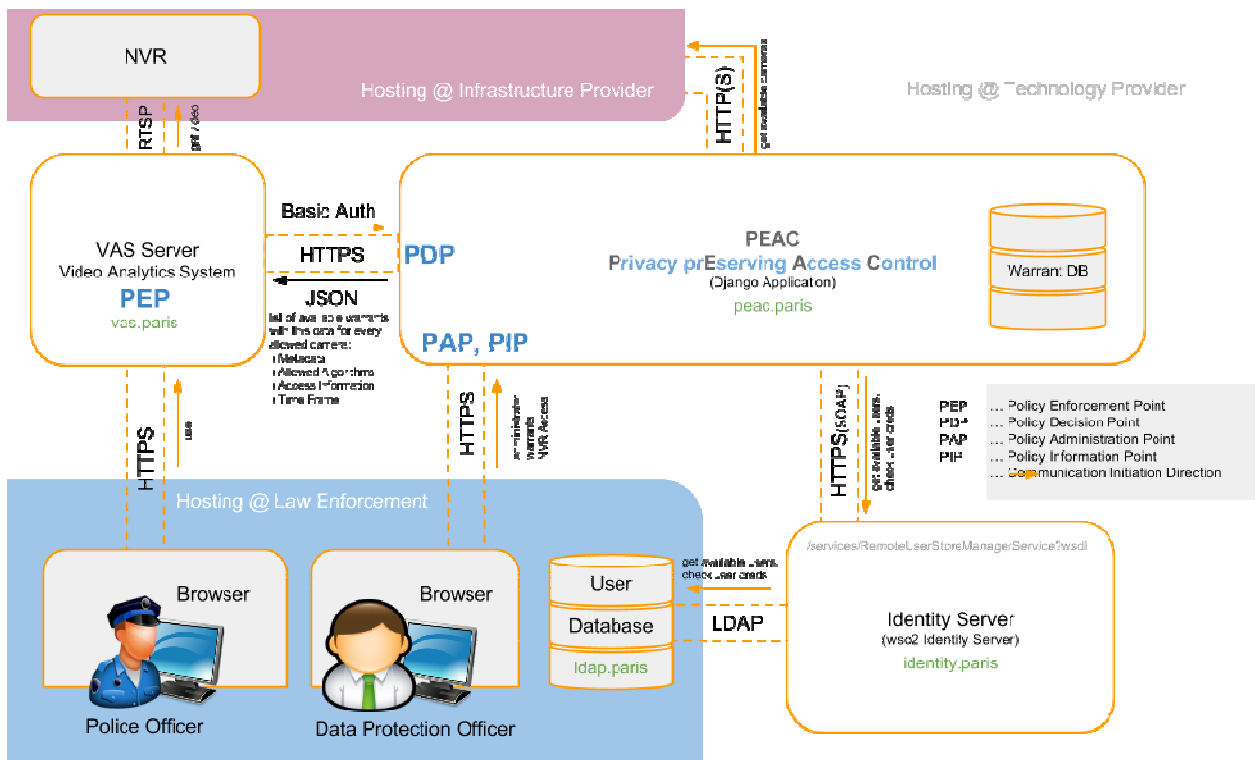


Figure 17 PEAC technical implementation view

## 4 Illustrated application of SALT processes and tools to the video-surveillance use case

The video-surveillance use-case provides application examples regarding the use and gains linked to the SALT tools and processes (and so does the biometrics use-case which is the subject of the WP6 of the project); also it will enable to evaluate the SALT tools and processes and to fine-tune them.

The video-surveillance use-case that has been defined in the previous deliverables of the project (mainly the D5.1 and the D5.2) has been chosen, according to the Description of Works, as relating to a system based on CCTV cameras installed in public places and operated by the Police for surveillance and crime prosecution (it might also be used in addition by other types of operators belonging to other agencies and for different purposes, such as a transportation regulation; the key point there is that the video-data are recorded and that they are at least partially accessed and used by the Police).

In addition to these definitions, and to provide sufficient information for the storytelling related to the use of the SALT tools and processes, the use-case is supposed to happen in France; this choice is not purely random, as French law provides precise constraints over the video-surveillance systems: this enables to easier exemplify the contents of the SALT framework.

The use-case is then provided with 2 different variations in order that privacy-related and accountability-related aspects are treated:

- The use case 1 “privacy-preserving law enforcement access to video archive search” is a privacy-related refinement,
- The use-case 2 “accountability of operators”, is an accountability-related refinement of the general use case.

These use-cases have been analyzed in the previous deliverables in order to scan the privacy and accountability issues at stake, and to draft when, by whom and to which outcomes the SALT tools and processes would be used. Also, this has been used to define the exact nature of the improvements and development of the new features that have been performed in the frame of the work-package (by Thales on the NVR, by AIT on the VAS, by Thales and AIT on the interfaces between the VAS and the NVR).

This means that the SALT process, and the outcomes of the process have already been scanned (because of the needs of the project). The goal of this section is to put things in chronological order by illustrating the use of the SALT tools to this use case, from the conception of the system to its use; by design, the outcomes of the process will point to the enhancements of the system that have been realized.

The figure below depicts a typical SALT process usage, with the identification of the different stakeholders who participate, and which information is produced by each, and subject to handover between the stakeholders.

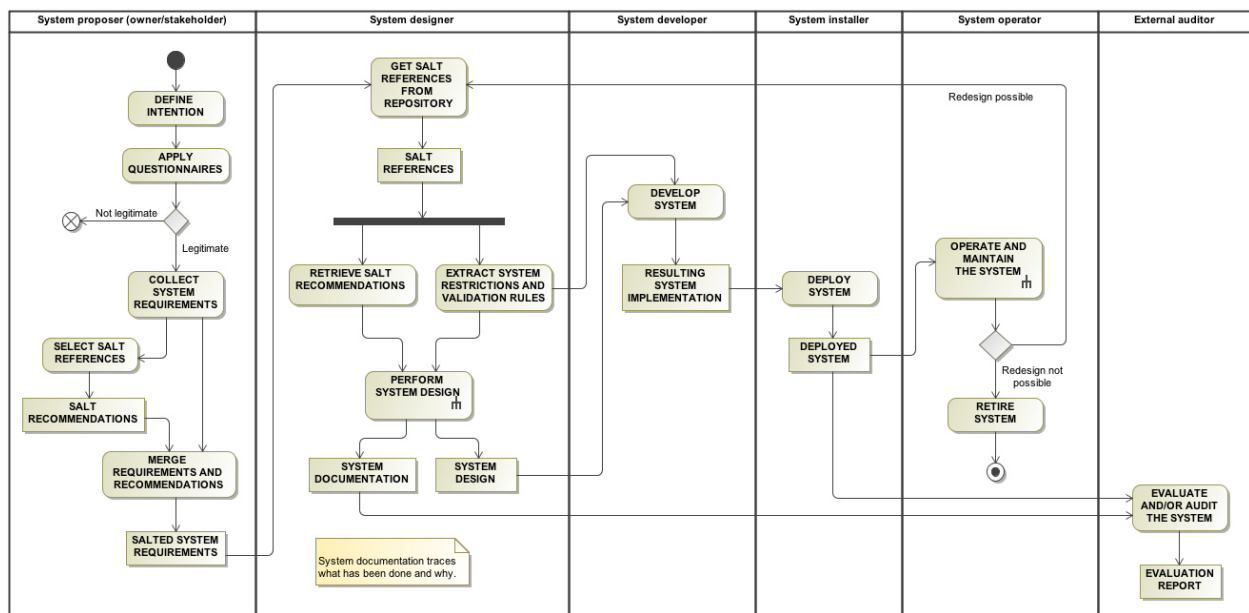


Figure 18: Typical process steps and stakeholders in the use of the SALT methodology

This figure represents the standard process; the activities and results might be a bit different in some real-life use-cases, where the responsibilities for each stakeholder could vary.

The following chapters illustrate, based on the above described standard SALT process, the use of the SALT tools applied to the video-surveillance use-case. This is performed for each of the stages of the process, with a description of the use of the SALT tools, and an overview of the typical results obtained at the end of the phase.

### 4.1 Overview about the use of the SALT tools

This part of the document is dedicated to the description of the use of the tools at the different steps of the lifecycle of the system: at intention phase, at design phase and at development phase. The use during the other phases of the project is then briefly described.

#### 4.1.1 System proposer SALT tools use description

The SALT proposer (who represents a team) sums up within the SALT repository and using the SALT tools the information about the intention and the need for the surveillance system. He also performs the selection of references that will orient the general specifications of the design; these references typically belong to the Legal specie (often providing some very general guidance about types of mechanisms that are mandatory or optional within the implementation of the system).

The main tasks the system proposer will perform through the SALT tools are:

- To answer the questionnaire,
- To select the references of interest,
- To write down some recommendations.

The typical outputs expected at this stage are detailed regarding the WP5 use case in §4.3.2.

### 4.1.2 System designer SALT tools use description

The system designer is the type of user intended to perform the design of the surveillance system. The system designer starts from the system specifications, requirements and constraints already identified during the intention phase of the process. This existing information comes as a result of the answers to the questionnaires, the SALT references already selected and the provided recommendations.

From this baseline, the designer enriches the contents of the SALT project:

- By selecting some new references (mainly technical references),
- By inputting some additional recommendations,
- By considering (eventually) the system model.

He may also, from this baseline, create a design for the current surveillance system, which is materialized in the form of an UML diagram. If privacy and accountability are important features to be met by the surveillance system, then adhering to the SALT process is a good decision to achieve a privacy-respectful system. In this case, the system designer can make use of a variety of tools to help him accomplish his task:

- The SALT repository: where all privacy and accountability information related to surveillance systems is stored. The information is organized in SALT references. Each reference may contain one or several privacy concerns. See Section 2.2.2.
- The UML profile: it provides a series of UML artifacts aimed to aid designers in the creation of an UML model of the system design. These artifacts cover video surveillance and biometric capabilities, as well as specific elements directly intended to fulfill privacy and accountability requirements.
- The automatic validator: this tool assists system designers during the creation of the system design model. If the SALT process is followed and information from SALT references is used to tackle with privacy and accountability requirements, the automatic validator can check, at design time, whether the concerns provided by the SALT references have been properly applied or not.

Apart from these tools, it is obvious that the system designer may also use any other parallel tooling specific to his/her company to perform design tasks. Now, according to the process flow described in Figure 18, we illustrate how a system designer makes use of the SALT tools.

This part of the document explains and illustrates how the system designer uses the SALT tools to perform these tasks. It also sums up the typical results that may arise from this phase.

In first place, the system designer receives the SALTed system requirements (issued mainly from the stakeholders and applicable legislation). We call them SALTed because after going through the first stage of the SALT process (checking convenient SALT references and answering the appropriate questionnaires), these requirements do not only relate to the system functionality, but also to privacy and accountability constraints the system should fulfill. With this information, the system designer can search the SALT repository in order to find those

references that are applicable to the current system under development, according to the type of system, localization, environment, etc. These new references, together with the initially provided specifications are what the designer needs to know to create a design.

At this point, the SALT methodology offers the aforementioned UML profile. This tool provides a list of artifacts that designers can use in their systems designs, helping them to tackle with the system constraints and to efficiently handle not only the functional requirements, but also privacy and accountability constraints. But how is this task carried out?

The UML profile also connects to the SALT repository and retrieves the SALT references the designer had searched (it provides an interface that allows for searching data in the repository). As mentioned, apart from the concerns descriptions, these references show some guidelines showing a possibility to implement the concerns' constraints into the system design. Of course, the designer may take the decision of not to follow such guidelines (let us remember that the whole SALT methodology is intended to aid users to create a privacy-respectful surveillance system, but it is not a decision making mechanism, humans always have the last word and they can choose whether they take into account the SALT methodology proposals or not).

In the case the guidelines are not followed, the developed tools cannot provide further assistance. However, if the designer pays attention to the proposed guidelines and apply them to the system design, then he can benefit from the automatic validator. This is another tool that runs on the background while the UML profile is being used. This validator has access to the OCL rules provided with the concerns of the selected SALT references. The OCL rules are formal ways of representing the proposed guidelines, and enable the tool to constantly check the system design model searching for inconsistencies. As a consequence if any OCL rule is not fulfilled at any time, it means that its corresponding guidelines have not been met, and then a message appears on the screen informing the designer about such violation.

Depending on the severity of the guidelines, the tool can pop out an error message, a warning or just some information to let the designer know. In any case, each message can be individually disabled for not bothering the designer in the case he decided not to follow the guidelines for a specific concern (he may prefer to approach the corresponding requirement from a different perspective he prefers).

Finally, at the end of this phase we expect an UML model with a design of the surveillance system under development. If the SALT process (and the above described tools) have been used, we can say this model represents a SALT compliant system design, where privacy and accountability requirements have been taken into account at the design stage, i. e. it fulfills the accountability and privacy-by-design approaches. Besides, the automatic validator also generates a report with relevant information about the system. This information depends on the SALT references used in the current system, thus each system will have different reports. What we can find in this document regards to what privacy and accountability concerns have been addressed, how they have been tackled in the system design, and why certain mechanisms and solutions have been implemented. All this information is very valuable for possible external auditors, among others.

Figure 19 shows an inside view of the system designer role, indicating the SALT tools he is intended to use, how they are interrelated and what are the inputs and outputs expected to be generated at the end of the workflow.

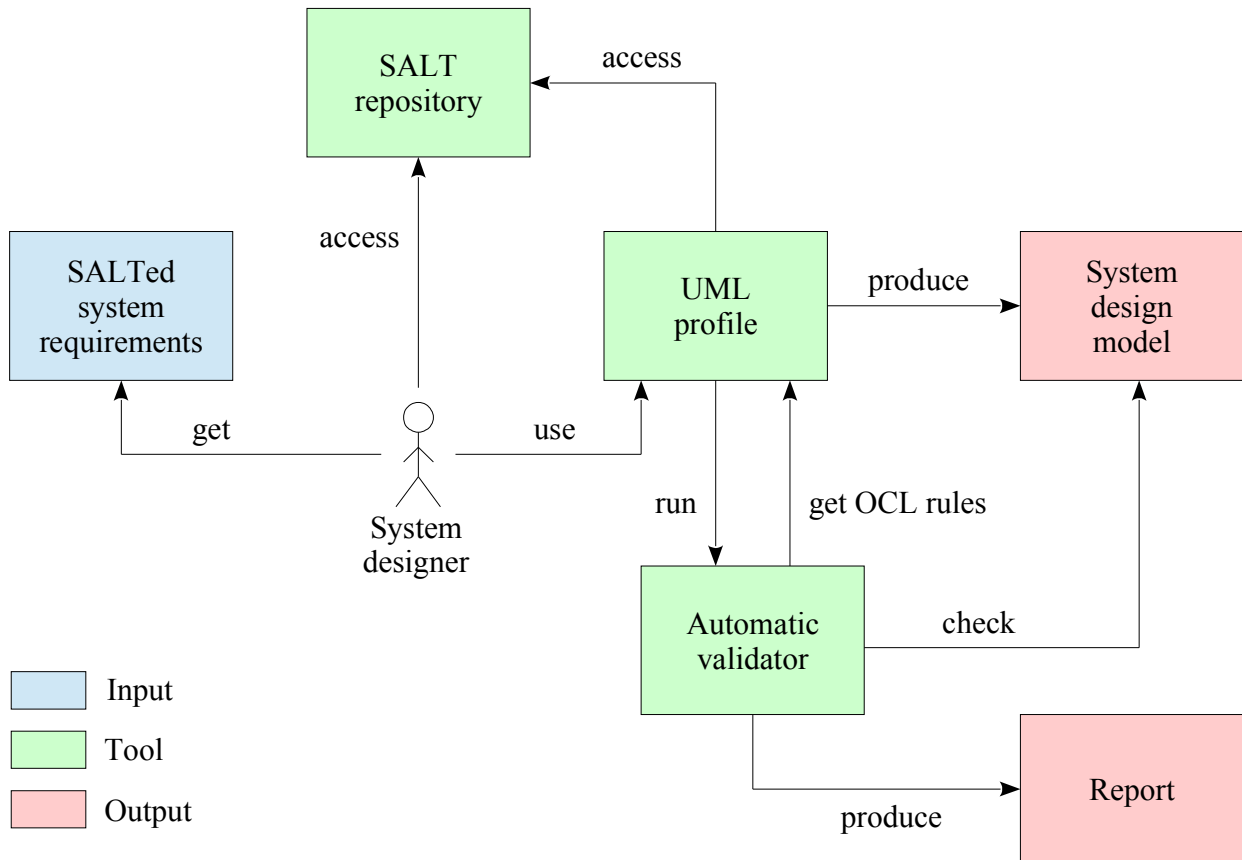


Figure 19. Usage of SALT tools for the system designer

### 4.1.3 System developer SALT tools use description

The development phase comes after the design phase. A presentation about the handover between different phases can be seen in Figure 18. System developers receive the system design generated by the designers, and this is the main document they have to follow. However, system developers also have access to more information, such as the system restrictions that were used during the design phase.

The above mentioned SALT tools have a less important role for system development. In general, system developers will use the tools they feel more comfortable with or those tools adopted by the company they belong to.

Nevertheless, they also have access to the information report generated by the automatic validator, so they are aware of the adopted solutions and mechanisms and their reason to be. This is important, since in case they decide to change some methods, they can check what constraints have been affected and act according to it. Moreover, they also keep access to the SALT repository, which allows them for consulting the desired SALT references in those cases the generated report is not sufficient.



At the end of the development stage, a full system implementation is provided, which will then be passed to the system installers. They will take care of the system deployment in a given environment, according to the original specifications.

#### **4.1.4 Other stakeholders potential use of the tools**

This part would be dedicated to the use of the SALT tools and contents especially during the operation and the maintenance of the system. 3 types of usages could be described:

- Re-use the SALT tools and contents the same way as a developer did: then the goal would be to check that the integrity of the system is maintained, or to cope with evolutions of the system that are to be handled using the SALT tools and processes (in this case, it consists of small loops of specification/design/development, which are comparable to these steps for the whole system),
- Apply the tools provided by the SALT to perform an assessment of a system that has not been specified, designed and developed using the SAT tools. In this case, the approach is close to the application of a Privacy Impact Assessment / Ethical Impact Assessment to the system. This approach is mainly based on a questionnaire, itself close to the ADVISE questionnaire proposed in the frame of the WP5 use-case,
- Apply the tools provided by the SALT at organizational level; then the SALT tools are used to perform an enquiry (close to an audit) related not really to the system itself, but to the way it is being used. This makes sense both in the case of a system developed using the SALT tools and not using them. In this case, the SALT applicable tool would be a questionnaire, slightly different from the one fed in the tools from the ADVISE project in the SALT tools.

## **4.2 Specificities of the use-case 1**

This part is dedicated to the use-case 1 (privacy preserving law enforcement access to video-archive search). As mentioned in section 4, there are two variations of the general use-case viewed from different perspectives. This section demonstrates how the SALT tools and processes are applied to a video surveillance system focusing on the privacy preserving aspect.

This is mainly covering:

- The identification at the questionnaire level of specific issues related to this use-case (risks and mitigation measures)
- One or several references that contains typical contents related to the analytics system and exports of video-surveillance footages,
- A link with the developments realized within the frame of the project (PEAC, etc.)

Real surveillance systems and the corresponding operation and video management are very diverse, which are specific to specific context, e.g. countries, usages, ownerships, and purpose etc. Therefore, our use case is oversimplified and made-up. It is also not the purpose of this use

case to show complex video analytic algorithms, but to demonstrate an instance of application of SALT framework to a video surveillance scenario. Under this premise it makes sense to select very basic algorithms involved in the use case and focus on the SALT framework and process.

### 4.2.1 Use case scenario

Below we present a refined and more “common sense” use case scenario, based on previous work in D5.2.

A ticket machine at a railway station has been broken twice during the last week. The method was the same and it is presumably that it was the same offender in both cases, so they are merged into one investigation. Unfortunately there is no video camera surveying the ticket machine, but there is a video surveillance of the elevator which is on the way to the ticket machine. Since the time of the crime cannot be determined exactly. For both cases there is a possible time window of about one hour during which the crime has been committed.

An investigation of the surveillance videos has been started. The objective of the investigation is to find persons that used the elevator on both days during the according time windows. To support the search by the means of video analytics, motion detection is used to compress the video to snippets where actual persons (or movements) are detected. Depending on the number of persons using the elevator, this can speed up the search time by magnitudes (see Figure 20).

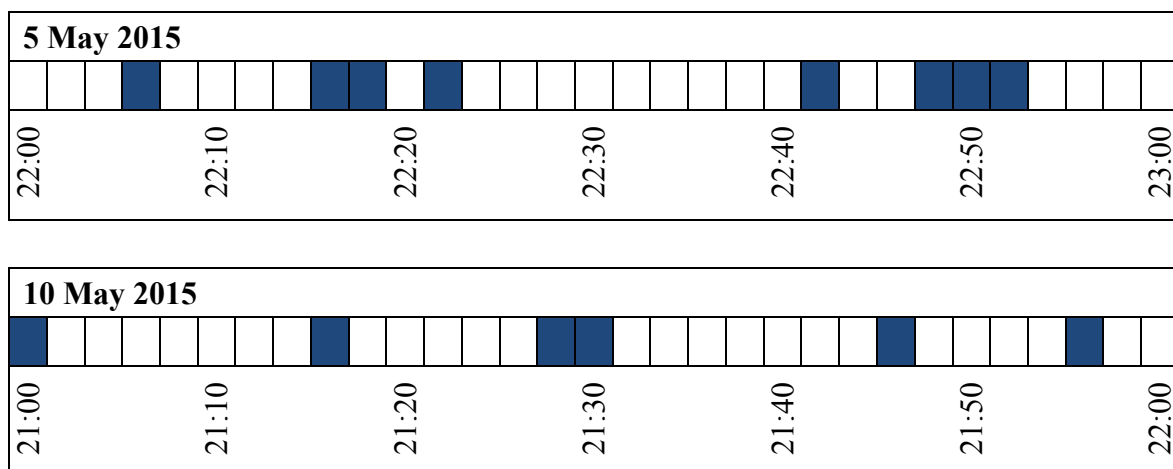


Figure 20 timeline of motion in surveillance video (marked blocks indicates the timeslots where motion was detected)

To provide the police officer in charge of the investigation with a better overview of the situation, a meaningful snapshot of each motion snippet is made and presented in a thumbnail overview. This makes it possible to show the detected persons of both days side-by-side (see Figure 21) and simplifies the search and comparison of the persons.



Figure 21 snapshots of detected motion in videos (sample images are taken from iLIDS video footage)

Once one or more suspects are identified, further investigations can be started. This could involve another video search or other criminalistic activities. However these further activities are out of scope of the demonstration use case of the PARIS project.

An automatic face evaluation has been left out consciously by two reasons. Until this point, no personal data have been extracted or computed from the video. An automatic face evaluation is a very strong algorithm in the sense of possible privacy impacts. The fact that such an algorithm would extract personal data of many innocent persons in the video makes it questionable if it is justified for this investigation, concerning the less privacy intrusive principle. The second – technical – reason is that not all faces of the persons in the video are visible in a way that they can be detected by automatic face detection and evaluation algorithms properly. The likelihood of false alarms / missed detections is quite high and makes this type of analytics not very useful for the given scene.

Concerning the WP5 video surveillance use-case the description of the investigation will stop at this point and the next section will continue with the description of the implementation of a privacy-preserving system according to the SALT processes.

#### 4.2.2 Privacy-preserving video analytics system

Figure 22 represents the main activities related to the privacy-preserving access control in use case 1.

### Police Officer Activity Diagram

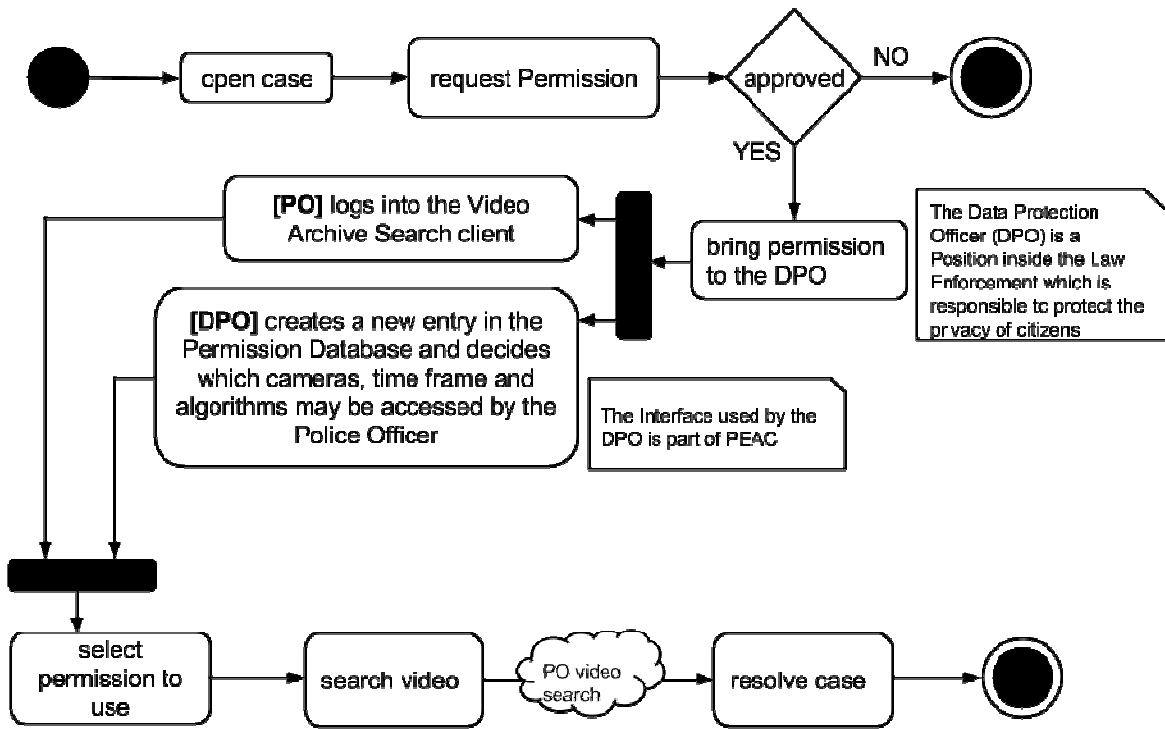


Figure 22 Activity diagram of the video analytics system use case

A warrant gives a police officer (PO) the permission to conduct an investigation using video analytics system. The warrant is the central object to PEAC. It can be seen as a policy or authorization entry. This object represents the warrant received from the judge or the direct authorization by the Data Protection Officer (DPO), depending on the applicable legal framework. Figure 23 shows the screen shot of the warrant as a record in the PEAC database.

Name	Users	Validity	Created	Modified
Recsepark Pickpocket	Investigator Phillip, Detective Johnson	15.12.2014 - 19.12.2014	DPO Smith, 8 minutes ago	DPO Smith, 7 minutes ago

Figure 23 A record of warrant in PEAC database

A permission implements the warrant in PEAC. The permission includes a combination of cameras with a shared time frame and algorithms. Within PEAC, it is seamlessly integrated into the warrant object, making it easier and more intuitive for the DPO to use the administration interface. Figure 24 shows the user interface for the DPO to edit the warrant.

The screenshot shows a web-based form titled "Change: Resselpark Pickpocket". The form contains the following fields and sections:

- Name:** Resselpark Pickpocket
- Users:** Investigator Phillips, Detective Johnson
- Valid from:** 15.12.2014
- Valid to:** 19.12.2014
- Active:** yes
- Permissions:**
  - Cameras:** Resselpark U-Bahn Eingang 1, Resselpark U-Bahn Eingang 2, Resselpark Restaurant, Resselpark Memorial, Resselpark Playground
  - Algorithms:** Body Contact, InvalidAlgorithm (highlighted with a red border)
- Time from:** 14.12.2014 16:00:00
- Time to:** 14.12.2014 17:00:00

At the bottom of the form, there is a red error message: "This data is invalid: InvalidAlgorithm". There are "Cancel" and "Save" buttons at the bottom right.

Figure 24 An example of the edit interface for permission in PEAC

The warrant includes the camera object. A camera object is used to identify surveillance camera tracks within an infrastructure provider, i.e. the owner or operator of a video surveillance system. The camera object has a name as well as an ID, which is used as a reference to identify the correct track when the video analytics system accesses the video data stored at the infrastructure provider to fetch and process the surveillance videos. Additionally they hold the (physical) camera address as well as its coordinates, these shall make selecting cameras more convenient. Figure 25 shows the graphic user interface for easily selecting cameras.



Figure 25 User interface for choosing cameras from a map

The providers describe Network Video Recorders (NVRs), which store the video data and are mostly located at the site of the surveillance cameras which they are used by. They have a name and hold arbitrary contact information. Technical information provided are the URL of the NVR, which only consists of the domain with an optional slug, in case the NVR is being proxied on a subdirectory when using RTSP over HTTP. Further Attributes are the RTSP port as well as the RTSP over HTTP port of the NVR and the Certificate or CA Certificate used by the NVR to enable CA/Certificate pinning. In the use case, we only consider that all video data is achieved at NVRs at a remote site. However, it is also possible to specify video data from other non-NVR sources.

The Algorithm object specifies the references algorithms used by the video analytics system. It is very simple, only consisting of a human readable name and its ID. The ID is used by the VAS to identify the algorithm in its own system.

A VAS-ID can specify a pre-configured combination of algorithms; this is used to overcome “the whole, is more than the sum of its parts” issue as it was briefly described at the end of section 3.3.1. Using this approach, the DPO (or a system administrator) can define allowed combinations of low-level computer vision algorithms as high-level algorithms for dedicated analytic purposes. On one hand, this has the advantage that all privacy related configurations and settings are done via the PEAC system. And on the other hand it increases the usability of the system for the police officer, since he does not need to struggle with technical details of low-level algorithms.

User objects are created if they are used in the database in order to link them to data for easier handling. They consist only of their Name and ID used in the external user storage. This enables

PEAC to easily connect to existing identity infrastructure, e.g. a LDAP or Active Directory of an enterprise IT system at a law enforcement site.

### 4.2.3 Reference / concern

A set of references are generated along the design and development of the use case, following the template introduced in **Section 2.2**.

The following references are identified to be relevant to the use case:

- Legal
  - Criminal Procedure Code (Strafprozeßordnung, StPO) on Seizure, Interception of Telecommunications, Computer-assisted Search, Use of Technical Devices, Use of Undercover Investigators and Search
- Technical
  - Logical access control to video surveillance systems
  - Scalability of video analytics
  - Detection quality of video analytics
  - Privacy risks management
  - Architecture patterns: access control for video archive search
  - Interoperability of authentication and identity management

Within the SALT process applied to the use-case 2, the legal reference here quoted is not purely prescriptive; however, it orients the team using the SALT tools to the selection of the technical references (that are then quoted following to the Legal one), in order to comply with the very generic requirements of the legal reference. This list of technical references contains precise technical features, which are implemented at design phase. The extensive contents of these references are found in Section 8.

## 4.3 Specificities of the use-case 2

As mentioned in section 4, there are two variations of the general use-case viewed from different perspectives. This section demonstrates how the SALT tools and processes are applied to a video surveillance system focusing on the accountability aspect.

This use case is related to the accountability of the operators. It has been built on an imaginary case where it is questioned whether or not an operator has viewed the live video stream produced by a camera at a given time; it is known that the video stream at this moment was showing a noticeable law infringement (such as the aggression of a person), that has not been signaled by any operator.

A comparable use case, with a different view of accountability is: a video from a CCTV filming a public space has been found on the internet; it should not have exited the system. The tools are used to find the operators who accessed the video.

This document part is mainly covering:

- The identification at the questionnaire level of specific issues related to this use-case  
The example identification of references that contains typical contents related to the archive search and exports of video-surveillance footages,
- A link with the developments realized within the frame of the project (PEAC, etc..)

### 4.3.1 Use case scenario

The second use case for the WP5 is similar to the first one; it nevertheless aims at focusing at accountability (and accountability by design as a result of the guidance provided by the SALT tools and methodology), whereas the first use case was most centered on privacy protection.

Within the two use-cases, the video-surveillance system is used to monitor an infrastructure with public access; the video-surveillance system provides live and recorded remote capabilities. Moreover, it provides special capabilities for the exportation of pieces of video footages: these video “records” or “clips” can be extracted from the system and played using standard video players (such as Windows movie player or VLC).

This type of video extract is especially suited for investigation and court prosecution; however it is most of the time (in most of the countries of the world, and especially within the European Union) strictly regulated and often dedicated only to Police operation and submitted to a judge requisition.

To illustrate the use case 2, a scenario is proposed, chosen to emphasize the complexity both of the video-surveillance systems and of their operational usage. The video-surveillance system is supposed to be deployed in a transportation infrastructure, typically a metro network, and used both by the metro operator for operational purposes (train positions and states, crowding level, dangerous behaviors of persons, who could be in position to be injured, working condition of devices of all kinds such as escalators) and by the Police, especially for forensics operations, with frequent needs for video data exports.



Figure 26 CCTV camera and typical image produced in a transportation infrastructure

This imaginary use case, which has been taken as a guiding example for the early elaborations performed within the WP2 of the project (the “Tabasco City” example) is not to be seen as a creation of the mind as it is exactly the configuration of the system used in the Paris (the French



City) RATP premises for the operation of the CCTV system: a single system is being used by both the Police and the metro operator in two adjacent rooms. Interesting facts are that the order of magnitude of monitored cameras is 5000, and the number of operator positions dedicated to Police is about 20. This ratio clearly points out that few live supervision is performed by the Police but rather forensics exploitation; the number of official requisitions (number of forensics cases) is several hundred per year with an explosive yearly growth.



*Figure 27: typical video operation room and video operators positions*

The use case 2 is dedicated to the accountability of the video operators of both types (Police and metro); two imaginary stories can be used to highlight this accountability, one from a “positive” bias, the other using a “negative” bias:

- The first case is brought by the submission of a complaint by a citizen, following an aggression that happened obviously within the field of view of a video-surveillance camera without any detection and reaction from the authority. The challenge is there to try to find if someone (and then who) have watched live the CCTV image.
- The second case is brought by the submission of a complaint by a citizen about CCTV image of his/her own person from CCTV cameras found on the internet. The challenge is then to try to find who (if anyone) acted as a breach and allowed the stealing and publication of the images,

Both of these sub use case variations are intended to underline and point out (through the SALT tooling) the technical means that could be used to identify the need for accountability mechanisms regarding the operator actions and behaviors, and to propose technological, organizational and operational solutions to this need.

The tools which are typically pointed out here as solutions to the operators accountability possible breaches is a log and audit mechanism within the NVR, dedicated to the operators actions (finer grain information is also provided thanks to the PEAC capability).

From the operational point of view, the administration of these tools and the access to their data (the operators' actions) is very sensitive, and most of the time restricted to few persons; the search and extraction of data would be performed e.g. on the requisite of a DPA (Data Protection Authority).

Last but not least, the demonstration of the features of the video system is performed using ILIDS files, which are certified by UK national body to cause no privacy harms.

#### **4.3.2 Example main outputs from SALT tools and processes**

The application of the SALT tools to the use case will be detailed and illustrated in the project next period deliverable (D5.4, Video Surveillance Lifecycle Management Use case evaluation). The main outputs expected from the SALT framework applied to the video-surveillance use-case are here detailed.

The figure below comes in addition to the Figure 18 (typical SALT process steps and stakeholders); the goal of these figures is to figure out the main SALT steps, stakeholders and expected outputs for each stage of the system development, from concept to retirement. The list of stages has been carefully examined, in order to provide information applicable to most of the system development process, which can widely vary depending on the type of organizations which are responsible for each of the steps.

	CONCEPT	DESIGN	DEVELOPMENT	DEPLOYMENT	OPERATION & MAINTENANCE	RETIREMENT
<b>GOALS</b>	Selection of the most suitable solution to solve the stakeholder's problem	Elaboration of the system design according to the different requirements	Implementation of the system based on the defined specification	Set up the biometric system in the stakeholder's environment	Use the system and ensure its correct functioning to satisfy stakeholder's needs	Shut down the system in a controlled manner
<b>COMMON TASKS</b>	<b>Collection of requirements</b> Identify stakeholders' needs Analyze possible solutions and viability	<b>Create solution description</b> Refine requirements Definition of procedures and responsibilities	<b>Build system</b> Integration of components Verify and validate system	<b>Install and configure the system</b> Inspect and test Training of end users	<b>Evaluation of system performance</b> System improvements and corrections End user support	<b>Store, dispose or archive the system</b> Analyze system interactions Determine retirement strategy
<b>SALT</b>	Define <b>purpose</b> and evaluate <b>legitimacy</b>	<b>Evaluate design:</b> Addressing SALT concerns?	<b>Evaluate development:</b> Addressing SALT concerns?	<b>Evaluate deployment:</b> Addressing SALT concerns?	<b>Periodic review of SALT concerns:</b> SALT concerns changed?	<b>Evaluate retirement:</b> Addressing SALT concerns?
<b>SALT Tools</b>	SALT Questionnaires		SALT References (prescriptive)			
		SALT Validation Tool	SALT References (non prescriptive: the guidelines)			
	SALT Taxonomies					

Figure 28: Lifecycle of SALT compliant systems

We do not consider here the whole video-surveillance system dedicated to public spaces, but rather we restrain to the privacy and accountability features underlined by the two use cases, within NVR and VAS sub-systems, especially in the case of Police forensics operations (privacy preserving capabilities put forward within the first use case, and accountability preserving capabilities regarding the second use-case).

At concept stage, the main tool used within the SALT framework would be the SALT questionnaire and SALT references. The goal of this step is to collect the main choices and requirements that weight on the system, while taking into account the legitimacy of the system and proportionality of the capabilities and measures it enforces compared to the goal of the system within its context of use.

The questionnaire which is used for the video-surveillance use-case is detailed within Annex A: ADVISE project PIA. The main questions that are related to accountability within this questionnaire are:

11. *Is the component/system interconnected with other components outside the system?*
12. *Is the information shared with other external systems? Does this component/system receive information from other external systems? Is the information lawfully obtained? What are the procedures for obtaining and transferring it?*
13. *Who has access to personal data processed by this component/system? What rights are assigned to each user?*
- 26.9. *How the will the transparency of this component/system be ensured?*

34. *What security measures for storage, transmission and access of the data are used?*
35. *What Privacy Enhancing Technologies (PETs) are employed?*
39. *What risks have been identified?*

The typical references that would be selected at concept stage are especially of Ethical and Legal type. The selection will vary with respect to the system and to the team using the SALT tools (the SALT selection being not unique), and especially with the country. If we locate the video-surveillance system in France, a typical reference that might be selected regarding this video-surveillance use-case would be the French ministerial decree of 3 August 2007 and its technical annex (cf. Section 8); quoting its concern "data sharing, technical requirements":

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

[...]

*- 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 on 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*

*O To know the identification of the camera, date and time of the record*

*O To search by camera, date and time*

[...]

Answering the questions and selecting this reference (in addition to other ones) is the core of the process that leads to a deterministic handling of accountability as a by-design approach, thanks to the SALT tools and methodology.

During the design phase of the video-surveillance system, the main SALT tool used is the reference, especially of technical specie. Gathering the already selected materials (questionnaires answers and choices, references selection at concept stage), the design is

obtained by precision and enhancement of these materials. Typically, the accountability mechanisms would enter the design phase thanks to the selection of the following reference at design stage: Logs and audit tools about operator actions for enhanced accountability.

*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.*

The design stage can also take benefit from a PIA (in the form of answering a SALT questionnaire) or from a refinement of a PIA performed at concept stage. Moreover, from a technical and engineering perspective, it is possible to draw a system model using normalized rules (typically UML, Uniform Modeling Language); on some conditions, it is possible to automate the verification that the design of the system matches some of the selected references prescriptions, using the automatic validation tool PAERIS (this ensures a compliance of a model to a set of references; this is of great interest).

The remaining stages (development, deployment, operation & maintenance, retirement) are handled by the SALT tools, but in a lighter form, as the goal is there to ensure that the decisions taken at concept and design times remain met. In the real-life of complex and long-duration systems, these additional steps may imply rework on the system; in a way, these are secondly-held concept and design sub-loops subject to the same type of SAT process already described.

### **4.3.3 Log and audit tools for enhanced accountability and their use**

In line with the operational need linked to the use-case, the development of the operator accountability tool (described in §3.2.2.3) has been performed within the NVR. It allows to search and browse, using multiple criteria, and from a web interface, the actions performed by the operators, including commands and controls realized on cameras.

The figure below points out, within the architecture of the VAS system, the position of the auditing tools.

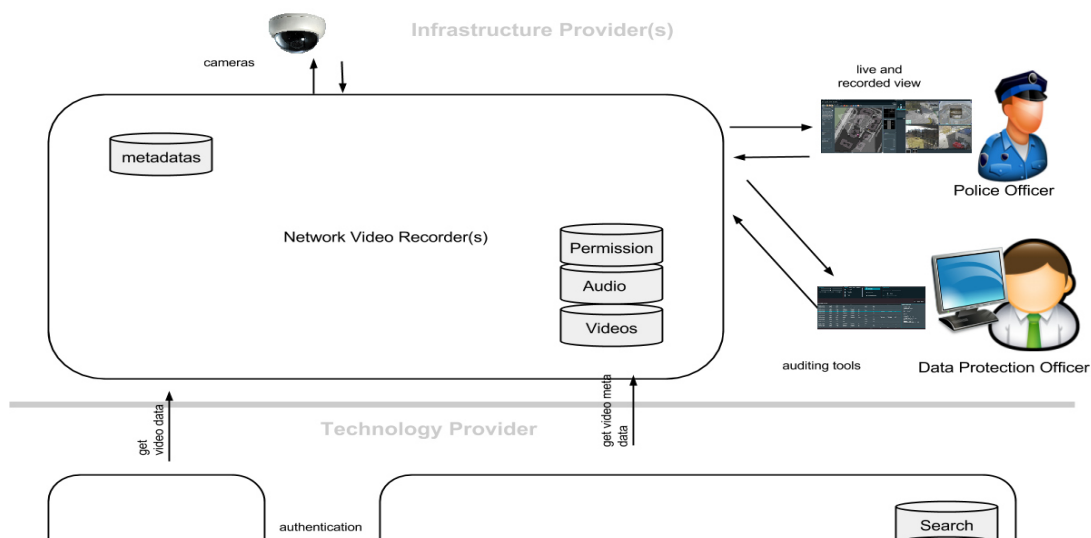


Figure 29 location of the NVR log and audit tools within the system architecture

The development that has been performed enables the DPA (or any other authorized person), to check the operator actions. This person would use the tool as following (in both use cases):

- Track back to the video sequence of interest (one or several); this is typically where the use of VAS (Video Archive Search) technologies can be used,
- Note the cameras and time of recordings for the sequences of interest,
- Log into the NVR auditing tool; perform a request about the cameras of interest, more specifically about the operator actions commutations of these cameras (a commutation is a command to display the video feed from the camera on the operator station or on a video wall),
- Note the list of operators that have commuted the camera on their screen within a given amount of time before the event of interest had happened.

In addition, the DPA (or equivalent person performing these operations) has the possibility to export safely the video footages of interest to external media, and to provide a mean to certify that these video footages are not altered from this point, using a capability developed into the Thales NVR within the PARIS project: hash-signage of the video export (hashes themselves encrypted using asymmetric cryptography), and a verification tool regarding the video-files integrity (described in §3.2.2.3).

[This procedure has to be performed in accordance with the national laws that prevail at the place of use of the system; using the SALT Framework however should enables to largely cope with the legality of this type of procedure].

## 5 Conclusion

This WP5 document comes in coherence with the preceding and future deliverables. In the previous WP5 documents (D5.1, Video Surveillance Lifecycle management Use case description, D5.2 Video surveillance Lifecycle management Use Case SALT compliant framework) the video-surveillance use case has been described from a technical point of view, and analyzed from privacy and accountability risks and PET (Privacy Enhancing Technologies) points of view. The D5.2 deliverable also provides SALT formatted contents in the form of references along each of the 3 SALT dimensions (Socio-ethical, Legal, Technological).

This D5.3 deliverable “video surveillance lifecycle management use case” brings together the use case technical and operational contents, the already computed SALT raw contents and the SALT tools and methodology in-line with their definitions performed within the WP3 and WP4 of the project. The SALT contents are augmented and refined, the SALT references are annexed in Section 8. The questionnaire, which is especially used in upstream phases of the SALT process has been computed from the PIA (Privacy Impact Assessment) that has been defined within the FP7 project ADVISE (Advanced Video Surveillance archive search Engine for security application). This PIA is especially suited to the PARIS WP5 case, as the underlying systems and surveillance technologies are exactly the same; the difference remains in the overall objective of the two projects. The ADVISE project focuses on the privacy issues related to video surveillance systems especially when dealing with Police forensics operations; the PARIS project uses this type of use case to exemplify and apply a generic process dedicated to privacy and accountability linked to any surveillance system. The ADVISE PIA is directly imported within the SALT repository using SALT tools: this is also a demonstration that the SALT processes and tools have defined approaches and information structuring compatible with existing material; this is an important statement, as the SALT appears then as a systematization, generalization (rather than a fully new approach that would need tremendous works to be operational) of processes that are already in place.

The video-surveillance use case is split within two sub use-cases, both applied using the same underlying system. The first use case is dedicated to the demonstration of the handling of privacy issues using the SALT tools and contents, and the second use case deals with taking into account accountability within the system. For both use cases, the system architecture and operational use are put forward by an imaginary operational scenario (however the scenarios are close to what happens in the real-life of teams and organizations using this type of system). For both use case, the outputs of the SALT tools are described and the consequent technologies or operational procedures prescribed are described. Some of the technologies are implemented concretely within a demonstration mockup that is common to AIT and Thales. This demonstration is described in this document, it is mainly based on a Network Video Recorder from Thales and on a Video archive Search from AIT together interfaced.

We arrive at this stage of the project to a refined use case, which enables to exemplify the SALT tools and processes from design to operation using 2 video-surveillance use-cases. The contents are now fed within the SALT tools developed by the WP3 of the PARIS project; from this concrete use, the SALT tools and processes will be assessed and the conclusions built into the next WP5 deliverable “Video Surveillance Lifecycle Management use case evaluation”.

## 6 References

ADVISE project (Advanced Video Surveillance archives search Engine for security applications) deliverable D2.4: "Monitoring reports on emerging ethical challenges in the developing and implementating the video archives. From J.Peter Burgess and Dariusz Kloza, VUB-IES.



## 7 Annex A: ADVISE project PIA

The PARIS project WP5 use cases are related to specific modules for video-surveillance systems, especially dedicated to surveillance of public spaces and used by public forces. This use case is very close to the one developed and nicely assessed in the ADVISE FP7 project (Advanced Video Surveillance archives search Engine for security applications).

The questionnaire reproduced below, and intended to be integrated in the PARIS project SALT Framework using the SFMT (SALT Framework Management Tools), is entirely reproduced from the deliverable D2.3 of the ADVISE project (Identification of practices and procedures of compliance for the use of video-surveillance archives); this deliverable was produced under the supervision of J. Peter Burgess and Dariusz Kloza from VUB (Vrije Universiteit Brussel). This questionnaire is hereby reproduced, and re-used in the PARIS project, under their written authorization.

### 7.1 General and technical description

**Name of the ADVISE component under assessment:**

**Name(s) of the assessor(s):**

**Date and place of the assessment:**

1. **Provide a brief overview of the component in question and its relation to other components and the system as a whole.**

*Please include a set of definitions for non-specialists.*

2. **What role does the component play in the system and what is its optimal outcome? By what means will this component achieve these goals?**

3. **What are, if any, the secondary functions of the component/system?**

*Secondary functions consider all these functionalities that the system/component can do on top of its main functions, i.e. those for which it was designed.*

4. **Role of the component. To what extent should the component be considered as necessary to the system? What alternative solutions exist?**

- 4.1. **To what extent should the component/system be considered as serving a legitimate aim as provided by law?**

*Generally speaking, interference with a human right is allowed if it serves at least one of the legitimate aims provided by law. With regard to the right to privacy, these are: national security, public safety, the economic well-being of the country, prevention of disorder or crime, protection of health or morals, the protection of the rights and freedoms of others.*

- 4.2. **Which use cases are these functionalities related to?**

*Please refer to the use cases defined in D3.1.*

- 4.3. **Which user/system requirements do these functionalities meet?**

*Please refer to the user requirements defined in D3.1 and the system requirements in D3.2.*

## **7.2 Description of information flows, including personal data**

### **5. What information is processed?**

*Please include a summary of information processed, regardless whether it is personal data or not. Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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.*

### **6. Does the component/system process personal data? What is the data? Does it include any sensitive data? Does it process biometric data?**

*Personal data mean any information relating to an identified or identifiable natural person (i.e. the data subject).<sup>2</sup>*

*An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.*

*Sensitive data is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and concerning health or sexual orientation.*

*Please provide a catalogue of personal data processed in the component/system.*

### **7. Does the component/system process meta-data? What is the meta-data?**

*Meta-data is 'data about data'. If it contains any information relating to an identified or identifiable natural person, meta-data is also considered personal data.*

### **8. What information, including personal data, is fed to the component/system? What is its source? Is the information lawfully obtained?**

### **9. What information, including personal data, is produced by the component/system? Which component is its destination?**

### **10. Is the component/system interconnected with other components *inside* the system?**

### **11. Is the component/system interconnected with other components *outside* the system?**

### **12. Is the information shared with other external systems? Does this component/system receive information from other external systems? Is the information lawfully obtained? What are the procedures for obtaining and transferring it?**

### **13. Who has access to personal data processed by this component/system? What rights are assigned to each user?**

### **14. What is the information, including personal data, used for?**

### **15. Is any information, including personal data, matched with any other information, including personal data? Does the processing of this information result in a creation of the profile of an individual?**

### **16. Insert one or more diagrams to illustrate how information, including personal data, is likely to 'flow' as a result of the functioning of the component.**

---

<sup>2</sup> For explanation, cf. Art. 29 Working Party, *Opinion 4/2007 on the concept of personal data*, Brussels, 20 June 2007, WP 136. [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf)

*PIA methodologies provide examples of data flow diagrams, e.g. the PIA template of the Office of the Victorian Privacy Commissioner.<sup>3</sup>*

### **7.3 Addendum: questions relating to the recording itself**

*These questions should be answered for the data used when ADVISE Consortium creates its own recordings for the purposes of research.*

**17. Please provide a brief overview of the content and format of the recording.**

**18. Are any areas monitored where expectations of privacy would be high?**

*These include, typically, individual offices (including offices shared by two or more people and large, open-plan offices with cubicles), leisure areas (canteens, cafeterias, bars, kitchenettes, lunchrooms, lounge areas, waiting rooms, etc.), toilet facilities, shower rooms and changing rooms.*

**19. Are any smart surveillance technologies employed?**

*Tools falling under this category include, among others: linkage of the video-surveillance system with biometric data (e.g. fingerprints for access control) or with any other database, whether biometric or not, or facial or other image recognition.*

**20. Is the quality of video relevant for the purposed surveillance (image, zoom, etc.)?**

*E.g. high-resolution might only be needed for face or car plate recognition. Sometimes only a fact of moving or lack thereof is relevant.*

**21. Is any covert surveillance employed?**

*Covert video-surveillance means surveillance using cameras that are either intentionally hidden from view, or are otherwise installed without appropriate notice to the public, and therefore it is reasonable to assume that the individuals monitored are unaware of their existence.*

**22. Is the video recording accompanied by audio recording?**

**23. Is any 'talking CCTV' employed?**

*'Talking CCTV' means any video-surveillance configuration using loudspeakers in the area under surveillance whereby the operators of the system can 'talk' to the members of the public who are under surveillance.*

**24. How are Individual rights assured?**

*Please answer the sub-questions directly.*

24.1. Are the individuals under surveillance notified of recordings being made?

24.2. Are the individuals under surveillance informed about the purpose of the recording?

24.3. Do individuals give free and informed consent to participate in the recording?

*Please clarify how consent is obtained. Please attach a model consent agreement or any other relevant document.*

24.4. Are the individuals able to access the information stored?

24.5. What are the redress procedures available for them, should they not agree with the procedures?

---

<sup>3</sup> Office of the Victorian Privacy Commissioner, *Privacy Impact Assessment Report*, template, April 2009, p. 9. <http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessment-report-template>

## 7.4 Risks identification

### 7.4.1 Risks related to ethics

#### 25. What ethical issues can this component/system raise?

*Please answer the sub-questions directly. Please refer to section 3.5 of the Deliverable D2.3 for further information.*

25.1. In what might the component/system, through its application, impact dignity, liberty or autonomy of the individual under surveillance?

*I.e. how might it harm or weaken an individual's feeling of self-worth, of belonging. How might it weaken an individual's or group's sense of its own access to the right and privileges proper to its culture and society?*

25.2. What harm might this component/system cause to the individual?

*I.e. how might it harm the individual in a physical way, but also in terms of its pride and humility? How might an individual's feeling of being a human being, endowed with rights and worth be weakened through disrespect, abuse or humiliation?*

25.3. What potential benefits will this component/system bring to the individual?

#### 26. What is the impact of this component/system on society?

*The ideal impact of applied security research is a more secure society, that is, an increase in the security of society obtained as a result of the research. Research is detrimental if it leads to the implementation of measures that either reduce the security of society or have no effect at all.<sup>4</sup>*

26.1. What documented societal security need(s) does this component/system intend to address?

*E.g. life, liberty, health, employment, property, environment, values.*

26.2. How will this component/system meet these needs? How will this be demonstrated?

*E.g. by processing information, organizing or redistributing resources, providing service, etc.*

26.3. What threats to society does this component/system address?

*E.g. crime, terrorism, pandemic, natural and man-made disasters, etc.*

26.4. How is this component/system appropriate to address these threats?

*E.g. how does it compare to other means of addressing the same needs, other services, resources, procedures or mechanisms.*

26.5. What segment(s) of society will benefit from increased security as a result of the functioning of this component/system?

*A wide range of different types of benefits may be produced from security research. Not all are relevant for all members of society. Thus, for example, improved emergency equipment represents an improvement of security for some segments of some societies but is far from globally beneficial.*

26.6. How will society as a whole benefit from this component/system?

---

<sup>4</sup> J. Peter Burgess, *The societal impact of security research*, PRIO Brief 9/2012. [http://file.prio.no/Publication\\_files/Prio/Burgess-Societal-Impact-Policy-Brief-9-2012.pdf](http://file.prio.no/Publication_files/Prio/Burgess-Societal-Impact-Policy-Brief-9-2012.pdf). Working Group on the Societal Impact of Security Research recently published its final report in which it presented a proposal for a *Checklist for Societal Impact of Security R&D Projects*.

*E.g. what collective or shared benefits does the component/system contribute to, how does it support society's overall traditions, values and aims?*

26.7. Are there other societal values that are enhanced by this component/system?

*E.g. other traits or characteristics of society that are of particular importance and which the component/system is intended to enhance?*

26.8. What is the political context of implementation of this component/system?

*E.g. how does the implementation complement or resist certain political programmes, orientations, government initiatives, etc.*

26.9. How will the transparency of this component/system be ensured?

*I.e. how will information about the system be made available with adequate support, analysis and explanation?*

26.10. How is the public likely to perceive the use of this component/system?

26.11. Is the component/system socially sustainable?

*Sustainability, in a conventional understanding, means that decisions made today should be defensible in relation to coming generations and the depletion of natural resources.*

## 7.4.2 Risks related to the right to privacy

**27. What types of privacy of the *individual* does this component/system potentially impact and how?**

*There are number of privacy types: privacy of a person, thought and feelings, of location and space, of data and image, of behaviour and action, and of communications.*

**28. How does this component/system potentially impact privacy of *association*, including *group* privacy?**

*Privacy of association (including group privacy), is concerned with people's right to associate with whomever they wish, without being monitored. This has long been recognised as desirable (necessary) for a democratic society as it fosters freedom of speech, including political speech, freedom of worship and other forms of association.<sup>5</sup>*

**29. How do the functionalities of this component/system potentially impact principle of necessity and proportionality?**

*In order for an interference with a protected right to be justified, the measure creating the interference: (i) must be appropriate to the fulfilment of the legitimate aim pursued, and (ii) it must not go beyond what is strictly required by the need to achieve that aim, i.e. it must be necessary to attain the objective justifying the interference). However, this second condition is sometimes described instead as requiring that the balance of interests has been respected. This alternative test – a balancing of interests, instead of a "strict necessity" test – will in particular be preferred where the aim pursued by the restriction was the protection of other fundamental rights, so that two values, of presumptively equal weight, come into conflict. Occasionally too, instead of being relaxed, the necessity test will be reinforced by the additional requirement that the aim pursued has a sufficient weight justifying the restriction.<sup>6</sup>*

*Please answer the sub-questions directly.*

<sup>5</sup> Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy", *European Data Protection: Coming of Age*, ed. S. Gutwirth et al., Dordrecht: Springer, 2013. [http://works.bepress.com/michael\\_friedewald/60](http://works.bepress.com/michael_friedewald/60)

<sup>6</sup> O. de Schutter, *International Human Rights Law. Cases, Materials, Commentary*, Cambridge 2010, pp. 313-314.

- 29.1. Is this component/system and its functionalities necessary in democratic society?
- 29.2. Are the functionalities of this component/system, listed in Question 4, relevant to its purposes?
- 29.3. Are the functionalities of this component/system, listed in Question 4, indispensable to satisfy the legal and technical requirements?
- 29.4. Are there less invasive solutions available? If yes, why they were not used?
- 29.5. Is this component/system, according to the state-of-the-art, an efficient tool to achieve its purpose?
- 29.6. Is the effectiveness of component/system regularly evaluated? How?

### 7.4.3 Risks related to the right to the protection of personal data

#### 30. How do the functionalities of this component/system impact the principle of data minimisation?

*Please answer the sub-questions directly.*

- 30.1. Is the personal data collected for specific, explicitly defined and legitimate purposes?
- 30.2. Is the data further processed in a way incompatible with those purposes?
- 30.3. What are the risks of function creep?

*Function creep is the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy.<sup>7</sup>*

- 30.4. What is the risk of dual use?

*Dual use goods are products and technologies normally used for civilian purposes but which may have military applications.<sup>8</sup>*

- 30.5. Are these personal data retained only for as long as is necessary to fulfil that purpose?

#### 31. How is the adequacy and accuracy of information, including personal data, assured?

*Please answer the sub-questions directly.*

- 31.1. How it is ensured that personal data are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed?
- 31.2. How it is ensured that personal data are accurate and, where necessary, kept up to date?

### 7.4.4 Risks related to other fundamental rights

#### 32. Are any other fundamental rights potentially affected, especially the right to fair trial, freedom of expression, freedom of assembly, freedom of religion, etc.? If so, how?

#### 33. Will the component/system and the information that comes out of it, directly or indirectly, contribute to the discrimination, stigmatization or stratification of social groups, based e.g. on ethnic origin or age?

---

<sup>7</sup> <http://dictionary.reference.com/browse/function+creep>

<sup>8</sup> <http://ec.europa.eu/trade/creating-opportunities/trade-topics/dual-use/>

*The system can implement with high precision protocols for discrimination (race, gender, class, etc.). This should be noted and flagged for potential analysis in a framework for law enforcement. For more information on discrimination, please refer to, inter alia, Handbook on European non-discrimination law (2011).<sup>9</sup>*

## 7.5 Risk assessment

### 7.5.1 Controls already implemented

#### 34. What security measures for storage, transmission and access of the data are used?

*What technical and organizational measures would be used to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing?*

*Security measures (controls) could be of technical or organisational nature. Technical controls are incorporated into the component through architectural choices or technically enforceable policies, e.g. default settings, authentication mechanisms, and encryption methods. Nontechnical controls, on the other hand, are management and operational controls, e.g. operational procedures.*

*Controls can be categorised as being preventive or detective. The former ones inhibit violation attempts and the latter ones warn of violations or attempted violations.*

#### 35. What Privacy Enhancing Technologies (PETs) are employed?

*PETs are systems of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system. These include, inter alia, encryption or access controls.*

#### 36. Is the personal data anonymised?

#### 37. How is the principle of privacy by default applied?

*Whenever reasonably possible, a high level of privacy protection should be provided automatically, so that no action is required from an individual to protect their privacy.*

#### 38. What other controls – that are not mentioned above – have been implemented?

### 7.5.2 Risk mitigation

*The methodology below is taken predominantly from the EU RFID PIA Framework. However, it is acceptable to use a different methodology. Please refer to Annex 1 for a list of privacy risk management methodologies.*

#### 39. What risks have been identified?

*Please provide a quantitative analysis of the risks identified. The risk assessment requires evaluating the applicable risks from a privacy, data protection and ethics perspective. It should be considered: (1) the significance of a risk, (2) the likelihood of its occurrence, and (3) the magnitude of the impact should the risk occur. Privacy risks may be high, medium or low.*

Risk ID	Risk description	Significance of the risk	Likelihood of occurrence	Magnitude of the impact	Comments
---------	------------------	--------------------------	--------------------------	-------------------------	----------

<sup>9</sup> <http://fra.europa.eu/en/publication/2012/handbook-european-non-discrimination-law>

---

--	--	--	--	--	--

**40. Are any residual risks left? Are they justified?**

*Following the assessment, one or more risks may remain. However, the benefits may be such that these risks are regarded as worth taking. Justification should be provided for such intrusion upon privacy and personal data.*

**7.6 Recommendations for the design of the component/system**

**41. Provide a set of critical recommendations with regard to the design of the component.**

*In particular, please focus on the controls to be implemented for each of the risks identified in Question 39.*

End of the questionnaire.



## 8 Annex B: SALT References for the video-surveillance Use Case

### 8.1 Introduction

This annex is produced as part of the WP5; it comes in addition and in complement to the D5.3 “Video-surveillance Lifecycle Management Use Case”.

The goal of the WP5 is to apply the SALT process and tools (defined and developed under WP2, WP3 and WP4 of the project) to a concrete video-surveillance use-case, to demonstrate the added value of the SALT processes and tools, and to provide an evaluation from this concrete use.

The SALT contents have been defined as embedding:

- SALT references, which are pieces of structured information with labels and description fields. The pieces of information can be of any of the 3 SALT pillar categories: Legal, Socio-Ethical, and Technical,
- SALT taxonomies, which are lists of words and terms referring to the domain of interest (here in PARIS WP5 to video-surveillance, and especially to video recording and video-analysis),
- SALT questionnaires, which are lists of questions (with explanations) that help decision makers describing their system, gathering the relevant information related to a given stage of a project (intention, design, build, operate).

Some references have already been defined within the D5.2 “Video Surveillance Lifecycle Management Use Case SALT compliant Framework” using a previous template.

This document sums up the applicable references defined in the scope of the project to the WP5. It contains:

- A first part related to the references template (which is identical to the template used for the WP6 work-package which addresses the biometrics use case,
- A second part dedicated to the references from WP5 itself (mainly based on the ones defined in D5.2),
- A third part which links the WP5 with the references defined in the analogous WP6 document: many of them are also applicable in the WP5.

The references listed in this annex are sorted in legal references, technical references, and socio-Ethical references (one chapter for each); it may happen that some references are cross-disciplinary: in this case, the reference is attached to the dominant domain it exhibits.

## 8.2 SALT References Template

This template summarizes all the information necessary to create a reference in the SALT Repository:

Field	Type	Description
<b>Reference name</b>	Mandatory	Name that serves to identify the reference, that should be as descriptive as possible. In case the references correspond to a law, an article, a report or any other official document, the name should be the title of that document.  In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen.  Example:  <i>Organic Law 15/1999 on the Protection of Personal Data - Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal</i>
<b>Original language</b>	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
<b>Abstract</b>	Optional	Brief summary of the contents of the reference (~ 100 words maximum)  In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields).
<b>Link to source</b>	Optional	Link to the source of information in the original language
<b>Link to translation</b>	Optional	Link to the source of information translated to English
<b>Official translation</b>	Optional	[Yes, No]  This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies).
<b>System type</b>	Mandatory	The system type to which the reference applies.  <i>Possible values: Video surveillance systems / Biometric systems / All systems</i>
<b>Geographical Scope</b>	Mandatory	A first layer of context information, which will define the territorial scope of application.  The SALT Framework Tool for the creation of references will provide a drop down list containing a set of predefined countries (by now, all the European countries and also the option "European Union" to cover all them).  There is also the option "Any" for the cases where this information is not relevant for the reference (e.g. technical information).
<b>Context</b>	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference (e.g. <i>specific cases/conditions where the reference is applicable</i> ).
<b>Version</b>	Mandatory	Version of the reference in the format vA.B.  By default this field has the value: v0.1
<b>Keywords</b>	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the reference
<b>Creator</b>	Automatic	Person responsible for the creation of the reference in the SALT Repository <i>(automatically filled by the SF Tool)</i>
<b>Last update</b>	Automatic	Date and time of the last reference update <i>(automatically filled by the SF Tool)</i>

<i>List of concerns (privacy and accountability related concerns for surveillance systems)</i>		
<b>Concern ID</b>	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
<b>Name</b>	Mandatory	<p>Title for the concern, which should give a brief idea of the contents or aspects covered by the concern.</p> <p>The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A text would probably include more than one concern.</p> <p>In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen.</p> <p>Example: Duty to inform - Deber de informar</p>
<b>Additional information</b>	Optional	Extra information that helps readers find the concern in the source text.
<b>Description</b>	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc.
<b>Category</b>	Mandatory	Category of the concern, that can be one or several among this options: <i>Legal, Socio-Ethical, Technical</i> .
<b>SALT Topics</b>	Mandatory	<p>SALT legal topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks.</p> <p>The list of defined SALT legal topics, and its mapping with the privacy principles indicated in ISO Standard 29100, is available in Reuse possibilities of the WP6 references</p> <p>An equivalent document to this one has been produced in the frame of the WP6: it contains an indicative list of references dedicated to the biometrics use-case. The biometrics system that is been especially focused on in PARIS is a soft-biometry system using cameras as sensor. For this reason, many guidelines of any specie (Socio-Ethical, Technical, Legal) may be applied to both of the systems types.</p> <p>This is of great interest because this also enables to show how the selection of applicable SALT data is realized for each of the use cases (among a consequent amount of available data): especially, SALT references are to be selected for each use case. A key selection parameter here will simply be the country where the use case is considered to be placed, as it is France for WP5 and Spain for WP6.</p> <p>All of the references that are listed in the WP6 document can be considered as valid for video-surveillance systems (for extensive contents of the references, please refer to the WP6 document), except those explicitly dedicated to biometrics systems, which are:</p> <ul style="list-style-type: none"> <li>• The Opinion 3/2012 on the development of biometrics systems,</li> <li>• Privacy by design solution for biometrics one-to-many identification systems</li> </ul>

Appendix C: Mapping of ISO principles and SALT legal topics		
<b>Stage</b>	Optional	<p>Stage or stages of the SALT Process in which this concern applies.</p> <p>These are the stages defined and their goals:</p> <ul style="list-style-type: none"> <li>• <b>concept</b> (intention): selection of the most suitable solution to solve the stakeholder's problem;</li> <li>• <b>design</b>: elaboration of the system design according to the different requirements;</li> <li>• <b>development</b>: implementation of the system based on the defined specification;</li> <li>• <b>deployment</b>: set up the system in the stakeholder's environment;</li> <li>• <b>operation &amp; maintenance</b>: use the system and ensure its correct functioning to satisfy stakeholder's needs;</li> <li>• <b>retirement</b>: shut down the system in a controlled manner.</li> </ul>
<b>Keywords</b>	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern.
<b>Guidelines</b>	Optional	Any guidance on how to include the concern in the development of the system. This could be a concrete artifact or solution, a strategy or procedure, or just any tip about how to take this concern into consideration.
<b>OCL Rules</b>	Optional	One or several OCL rules that allow to verify that the system addresses the concern. The OCL expert needs to fully understand the meaning of the privacy/accountability concern for which the OCL rules are created. These rules will be used for the automated (or human assisted) validation of the concern it relates to, once its corresponding solution provided by the SALT reference has been implemented in the system design.

To take into consideration:

- 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 SALT repository can store two types of SALT references:
  - **Complete SALT Reference**: that include OCL rules for one or many concerns.
  - **Standard SALT reference**: the reference lacks of the information regarding OCL rules.
- Since every concern may correspond to one (or several) stage within the SALT process, we have decided to include a new field in the repository for each concern. This new field will keep track of the stage to which a given concern may apply. How the automatic validator behaves when dealing with a concern, depends on the stage of such concern:
  - Design stage: the automatic validator imports the OCL rules (if any) and check whether they are fulfilled (the system design follows the guidelines proposed by the SALT reference) or not. As a result, this information can appear in the generated report.
  - Any other stage different from design: the automatic validator works at design time over a UML diagram (a model of the system design). Therefore, those concerns not applicable to the design stage fall out of its range of action. However, it still can retrieve the guidelines provided by such concerns and copy them to the generated report. In this way, the report can be structured in a way

that clearly shows each stage and what concerns (out of the design stage) have to be taken into account for every stage. This information will be of importance for future users of the system after its design

### 8.3 SALT References for the Video-Surveillance Use Case

The references here described are mainly issued from the D5.2, and reformatted to match the more elaborated format defined for the references. A few references that appeared of lesser interest have not been reused; some references will also be added.

Note that not all the references listed here are applicable to the video-surveillance use-case; one of the key features of the SALT tools is to allow the selection of the applicable references in a given case; this will enable to demonstrate this feature.

#### 8.3.1 Legal SALT references for the video-surveillance use-case

References description. Fields	References descriptions
Reference name	<b>Belgium Law on video-surveillance 2007 (amended 2009)</b>
System type	video-surveillance systems
Geographical scope	Belgium
Reference name	<b>Information Commissioner's CCTV Code of Practice</b>
System type	video-surveillance systems
Geographical scope	United Kingdom
Reference name	<b>French homeland security code - video-surveillance in public spaces</b>
System type	video-surveillance systems
Geographical scope	France
Reference name	<b>French homeland security code - video-surveillance in publicly accessible premises</b>
System type	video-surveillance systems
Geographical scope	France
Reference name	<b>French homeland security code – Fight against terrorism - video surveillance</b>
System type	Video-surveillance systems
Geographical scope	France
Reference name	<b>technical requirements from French ministerial decree of 3 August 2007</b>
System type	Video-surveillance systems
Geographical scope	France
Reference name	<b>French Code of Criminal Procedure - (art. 60-1, 77-1-1, 93-3)</b>
System type	All

<b>Geographical scope</b>	France
<b>Reference name</b>	<b>French Data Protection Act (Act n°78-17 of 6 January 1978)</b>
<b>System type</b>	All surveillance systems
<b>Geographical scope</b>	EU
<b>Reference name</b>	<b>EU Law Enforcement Data Protection Directive Proposal (pending legislative act – not approved)</b>
<b>System type</b>	All
<b>Geographical scope</b>	EU
<b>Reference name</b>	<b>EU data Protection Regulation Proposal (not approved yet)</b>
<b>System type</b>	All surveillance systems
<b>Geographical scope</b>	EU
<b>Reference name</b>	<b>Criminal Procedure Code (Strafprozeßordnung, StPO) on Seizure, Interception of Telecommunications, Computer-assisted Search, Use of Technical Devices, Use of Undercover Investigators and Search</b>
<b>System type</b>	Video-surveillance systems
<b>Geographical scope</b>	Austria

### 8.3.1.1 Access to images by law-enforcement authorities in Belgium

<b>Reference name</b>	<b>3.1.1 Belgium law on video-surveillance 2007 (amended 2009)</b>
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Belgium
<b>Context</b>	All stages
<b>Version</b>	0.1
<b>Keywords</b>	public roads, market places, streets, squares, parks, shops, banks, restaurants, cafés, cinema
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Access request by law enforcement authorities
<b>Additional information</b>	data sharing, disclosure

<b>Description</b>	<ul style="list-style-type: none"> <li>- The controller <b>can</b> (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.<sup>10</sup></li> <li>- The controller <b>shall</b> transmit, free of charge, the images to police authorities acting in the course of their missions of administrative police or judicial police <u>on their request</u>.</li> </ul>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal Basis
<b>Stage</b>	All stages
<b>Keywords</b>	
<b>Guidelines</b>	The system design must have an element (usually a method) marked with the stereotype «data_transmission_process», which represents the procedure that allows for transmitting data (to police services or judicial authorities).
<b>OCL Rules</b>	context Class inv Concern LawBelgium.1 ParisProfile::Legal::Data_transmission_process::allInstances()->size()>=1
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Access request from law-enforcement authorities
<b>Additional information</b>	
<b>Description</b>	<ul style="list-style-type: none"> <li>- The controller <b>can</b> 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.</li> <li>- The controller <b>must</b> transmit, free of charge, the images to police authorities acting in the course of their missions of judicial police, <u>on presentation of a judicial warrant</u>.<sup>11</sup></li> </ul>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal Basis
<b>Stage</b>	From concept to operation
<b>Keywords</b>	
<b>Guidelines</b>	<p>The system design must have an element (usually a method) marked with the stereotype «data_transmission_process», which represents the procedure that allows for transmitting data (to police services or judicial authorities).</p> <p><i>[This is equal to the previous concern, we can ensure to provide a mechanism for data transmission, but it is not possible to automatically decide whether the recorded images have an evidential value or not].</i></p>
<b>OCL Rules</b>	context Class inv Concern LawBelgium.1 ParisProfile::Legal::Data_transmission_process::allInstances()->size()>=1

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

<b>Reference name</b>	<b>3.1.1 Information Commissioner's CCTV Code of Practice</b>
-----------------------	---

<sup>10</sup> Article 9 1° of the law on video surveillance

<sup>11</sup> Article 9 2° of the law on video surveillance

<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	United kingdom
<b>Context</b>	All stages
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Access to images
<b>Additional information</b>	data sharing, disclosure
<b>Description</b>	<p>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.”</p> <p>“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.”</p> <p>“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.</p> <p>Images can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.</p> <p>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.”</p> <p>“Judgements about disclosure should be made by the organisation operating the CCTV</p>



	<p>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.</p> <p>The method of disclosing images should be secure to ensure they are only seen by the intended recipient.”</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal Basis
<b>Stage</b>	Design, development, operation
<b>Keywords</b>	
<b>Guidelines</b>	<p>Elements of the system with access to data must be related to at least two other elements:</p> <ul style="list-style-type: none"> <li>• One associated to the stereotype «control_access». This element restricts access to the elements that can access data.</li> <li>• Another associated to the stereotype «produce_log_entry». This element is intended to add a log entry each time data is handled.</li> </ul> <p>There must exist an element in the system associated to the stereotype «autodeletion». This element is in charge of removing data that is no longer needed (expiration date arrival).</p> <p>Elements of the system intended for data disclosure (they could also be considered as elements for data transmission) have to be associated to the stereotype «security_mechanisms». This stereotype has a list type attribute, where each element of the list is a text string, containing the security mechanisms applied to the data disclosure procedure.</p>
<b>OCL Rules</b>	<p>LawUK.1</p> <p>context Class inv Concern LawUK.1</p> <p>ParisProfile::Legal::Autodeletion::allInstances()-&gt;size()&gt;=1</p> <p>LawUK.2</p> <p>context Class inv Concern LawUK.2</p> <p>self.ocllsTypeOf(ParisProfile::General::Control_Access) and self.ocllsTypeOf(ParisProfile::Legal::Produce_log_entry)</p> <p>LawUK.3</p> <p>context Class inv Concern LawUK.3</p> <p>self.ocllsTypeOf(ParisProfile::Legal::Security_mechanism) and self.oclAsType(ParisProfile::Legal::Security_mechanism).list-&gt;notEmpty()</p>

### 8.3.1.3 French homeland security code

The regulation of video surveillance in France mainly follows from two laws. The Act on Information Technologies and Civil Liberties ('Loi Informatique et Libertés')<sup>12</sup> 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'<sup>13</sup> as amended, the provisions of which can now be found in the Homeland security code. The French "code de la sécurité 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).

Reference name	Access to images by law enforcement authorities in Belgium
Original language	French
Abstract	
Link to source	
Link to translation	Unofficial translation
Official translation	
System type	Video-surveillance systems
Geographical Scope	France
Context	
Version	0.1
Keywords	Video surveillance of public spaces, Parks, streets, public roads, open markets, highways
Creator	NAMUR
Last update	20/12/2014
<i>List of concerns</i>	
Concern ID	TBD (SFMT)
Name	article L251-1 and following (partial)
Additional information	
Description	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;

<sup>12</sup> 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

<sup>13</sup> 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

	<p>4) Detection of road traffic offences;</p> <p>5) Prevention of offences against people or goods;</p> <p>6) Prevention of terrorist acts according to article L223-1 and following of the Homeland security Code;</p> <p>7) Prevention of natural or technological disasters;</p> <p>8) Emergency assistance to individuals and fire protection;</p> <p>9) Safety of installations in amusement parks.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal Basis, purpose specification
<b>Stage</b>	Concept
<b>Keywords</b>	intention, Purpose legitimacy and specification
<b>Guidelines</b>	
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	article L251-1 and following (partial), publicly accessible premises
<b>Additional information</b>	
<b>Description</b>	<p>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.</p> <p>They can also be installed when subject to terrorist threats (see Ref. Homeland security Code – Fight against terrorism – video surveillance)</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	intention, Purpose legitimacy and specification
<b>Stage</b>	concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	article L252-5, maximum duration of video-footages retention
<b>Additional information</b>	
<b>Description</b>	<p>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.</p> <p>[...]</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	intention, Purpose legitimacy and specification
<b>Stage</b>	Concept, design
<b>Keywords</b>	
<b>Guidelines</b>	Elements of the system representing video-surveillance recordings must be attached to the stereotype «video_surveillance_recording». This stereotype has at least one attribute:

	<ul style="list-style-type: none"> <li>«expiration_date»: this attribute defines the maximum period of time the recorded data can be stored before it is deleted by the autodeletion mechanism. This period will typically be of one month, except for the cases shown in the description above.</li> </ul> <p><i>[The OCL rule will check the existence of the «video_surveillance_recording» stereotype (with the inherent «expiration_date» attribute), but it can do nothing to check the retention period of data (one month or more), since it is not possible for a rule to automatically detect whether the data is considered an exception or not.]</i></p>
<b>OCL Rules</b>	<p><b>LawFrance.1</b> context Class inv LawFrance.1 ParisProfile::Legal::Video_surveillance_recording::allInstances()-&gt;size()&gt;=1</p> <p><b>LawFrance.2</b> context Video_surveillance_recording inv LawFrance.2 not self.expiration_date.ocllsUndefined()</p>

#### 8.3.1.4 French ministerial decree of 3 August 2007 and its technical annex

<b>Reference name</b>	<b>Access to images by law enforcement authorities in Belgium</b>
<b>Original language</b>	French
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	Unofficial translation
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	France
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	data minimisation, orientation of cameras
<b>Additional information</b>	

<b>Description</b>	<p>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 or post-processing enable to reach the security objective for which the system has been installed.</p> <p>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.</p> <p>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.</p> <p>[...]The second consequence is that the technical features of the cameras shall enable to reach the goals of the system.</p> <p>[...]</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Fairness, legal basis, purpose specification, data minimization
<b>Stage</b>	Concept, design, installation
<b>Keywords</b>	video surveillance in public spaces, video surveillance in publicly accessible spaces
<b>Guidelines</b>	
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Data sharing: technical requirements
<b>Additional information</b>	
<b>Description</b>	<p>The exportation of images (sharing with law enforcement authorities) from systems of video surveillance is subject to technical requirements:</p> <ul style="list-style-type: none"> <li>- Surveillance cameras with narrow fields of view shall have a format greater than or equal to 704 x 576 pixels.</li> <li>- 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.</li> <li>- A minimum of 12 images per second for cameras with narrow fields of view</li> <li>- A minimum of 6 images per second for other cameras with wide fields of view</li> <li>- 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</li> <li>- 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</li> <li>- The video surveillance system must continue to record during the operation of exportation</li> <li>- The images exported are stocked on a non-rewritable system (in general they will be burned on 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.</li> <li>- The software to exploit the images must also be transmitted to the police. It must allow: <ul style="list-style-type: none"> <li>o To read the records without reduction of images' quality</li> <li>o To read the records over cranking and under cranking</li> <li>o To read image by image</li> <li>o To know the identification of the camera, date and time of the record</li> <li>o To search by camera, date and time</li> </ul> </li> <li>- [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]</li> </ul>

	<table border="1"> <thead> <tr> <th data-bbox="427 190 837 248">SITUATION</th> <th data-bbox="837 190 965 248">RÉSOLUTION minimum de l'image stockée</th> <th data-bbox="965 190 1093 248">NOMBRE D'IMAGES par seconde au minimum</th> <th data-bbox="1093 190 1321 248">COMMENTAIRES classification plan étroit/plan large</th> </tr> </thead> <tbody> <tr> <td data-bbox="427 248 837 309">Caméra de surveillance de la voie publique en agglomération aux abords d'un site sensible.</td> <td data-bbox="837 248 965 309">CIF</td> <td data-bbox="965 248 1093 309">6</td> <td data-bbox="1093 248 1321 309">Plan large.</td> </tr> <tr> <td data-bbox="427 309 837 353">Caméra de surveillance d'un monument sur la voie publique</td> <td data-bbox="837 309 965 353">CIF</td> <td data-bbox="965 309 1093 353">6</td> <td data-bbox="1093 309 1321 353">Plan large.</td> </tr> <tr> <td data-bbox="427 353 837 398">Caméra de surveillance d'un automate (DAB...).</td> <td data-bbox="837 353 965 398">4 CIF*</td> <td data-bbox="965 353 1093 398">6</td> <td data-bbox="1093 353 1321 398">Plan étroit.</td> </tr> <tr> <td data-bbox="427 398 837 443">Caméra de surveillance à l'intérieur d'un véhicule de transport public.</td> <td data-bbox="837 398 965 443">4 CIF*</td> <td data-bbox="965 398 1093 443">6</td> <td data-bbox="1093 398 1321 443">Plan étroit.</td> </tr> <tr> <td data-bbox="427 443 837 488">Caméra de surveillance sur un quai de gare.</td> <td data-bbox="837 443 965 488">CIF</td> <td data-bbox="965 443 1093 488">6</td> <td data-bbox="1093 443 1321 488">Plan large.</td> </tr> <tr> <td data-bbox="427 488 837 584">Caméra de surveillance en entrée ou sortie d'un commerce, d'un musée, d'une agence bancaire, d'un lieu ouvert au public.</td> <td data-bbox="837 488 965 584">4 CIF*</td> <td data-bbox="965 488 1093 584">12 ou 6</td> <td data-bbox="1093 488 1321 584">Plan étroit 6 si un dispositif de filtrage des flux de personnes est présent (sas, tourniquet...).</td> </tr> <tr> <td data-bbox="427 584 837 629">Caméra de régulation du trafic routier</td> <td data-bbox="837 584 965 629">CIF</td> <td data-bbox="965 584 1093 629">6</td> <td data-bbox="1093 584 1321 629">Plan large.</td> </tr> <tr> <td data-bbox="427 629 837 674">Caméra de surveillance d'un comptoir ou d'un guichet.</td> <td data-bbox="837 629 965 674">4 CIF</td> <td data-bbox="965 629 1093 674">6</td> <td data-bbox="1093 629 1321 674">Plan large.</td> </tr> <tr> <td data-bbox="427 674 837 719">Caméra de surveillance de rayons d'un magasin.</td> <td data-bbox="837 674 965 719">CIF</td> <td data-bbox="965 674 1093 719">6</td> <td data-bbox="1093 674 1321 719">Plan large.</td> </tr> <tr> <td data-bbox="427 719 837 763">Caméra de surveillance d'une pompe de carburant.</td> <td data-bbox="837 719 965 763">4 CIF*</td> <td data-bbox="965 719 1093 763">6</td> <td data-bbox="1093 719 1321 763">Plan étroit.</td> </tr> <tr> <td data-bbox="427 763 837 808">Caméra de surveillance d'une caisse ou d'un terminal de paiement.</td> <td data-bbox="837 763 965 808">4 CIF*</td> <td data-bbox="965 763 1093 808">6</td> <td data-bbox="1093 763 1321 808">Plan étroit.</td> </tr> </tbody> </table>	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, tourniquet...).	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.
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, tourniquet...).																																														
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.																																														
<b>Category</b>	Legal																																																
<b>SALT Topics</b>	Data quality, legal basis																																																
<b>Stage</b>	Design																																																
<b>Keywords</b>	Images resolution, metadatas																																																
<b>Guidelines</b>	<p>The stereotype «data_exportation» (associated to the system elements that physically export images, which is different from a digital data transmission) has the following attribute:</p> <ul style="list-style-type: none"> <li>• «camera»: it indicates which camera performs the data exportation.</li> </ul> <p>The corresponding OCL rules check that the camera resolution is greater or equal to 704 x 576 pixels and the frame rate is 12 fps or greater for cameras with a narrow field of view. For cameras with a wide field of view, the OCL rules will check for a resolution of at least 352 x 288 pixels and a frame rate of 6 fps or higher.</p> <p>Moreover, the element with the stereotype «data_exportation» must be related to another element with the stereotype «produce_log_entry», otherwise it will have the stereotype «produce_log_entry» together with the stereotype «data_exportation». The stereotype «produce_log_entry» has the following list of boolean (true or false) attributes:</p> <ul style="list-style-type: none"> <li>• «list_of_images»</li> <li>• «images_date_and_time»</li> <li>• «duration»</li> <li>• «cameras_identification»</li> <li>• «exports_date_and_time»</li> <li>• «user_identity»</li> </ul> <p>The OCL rules will check that all these attributes are set to «true», indicating all this information is recorded into the log.</p> <p><i>[Regarding the images' quality, an OCL rule is unable to determine whether the quality has been lowered or not, even more after compression.</i></p> <p><i>The rest of the concern description is related to the operation phase and cannot be checked by an OCL rule (for example, a rule cannot guarantee that a system operator will use a DVD to record images).]</i></p>																																																

<b>OCL Rules</b>	<p>LawFrance.3 context Class inv LawFrance.3 ParisProfile::Legal::Data_exportation::allInstances()-&gt;size()&gt;=1</p> <p>LawFrance.4 context Data_exportation inv LawFrance.4 not self.camera.oclsUndefined()</p> <p>LawFrance.5 context Data_exportation inv LawFrance.5 (not self.camera.oclsUndefined()) and self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).field_of_view=ParisProfile::Types::ViewType::narrow implies self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).resolution_width&gt;703 and self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).resolution_height&gt;575 and self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).fps&gt;11</p> <p>LawFrance.6 context Data_exportation inv LawFrance.6 (not self.camera.oclsUndefined()) and self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).field_of_view=ParisProfile::Types::ViewType::wide implies self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).resolution_width&gt;351 and self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).resolution_height&gt;287 and self.camera.oclAsType(ParisProfile::VideoSurveillance::Camera).fps&gt;5</p> <p>LawFrance.7 context Data_exportation inv LawFrance.7 (not self.log.oclsUndefined()) and self.log.oclAsType(ParisProfile::Legal::Produce_log_entry).list_of_images=true and self.log.oclAsType(ParisProfile::Legal::Produce_log_entry).images_date_and_time=true and self.log.oclAsType(ParisProfile::Legal::Produce_log_entry).duration=true and self.log.oclAsType(ParisProfile::Legal::Produce_log_entry).cameras_identification and self.log.oclAsType(ParisProfile::Legal::Produce_log_entry).exports_date_and_time=true and self.log.oclAsType(ParisProfile::Legal::Produce_log_entry).user_identity=true</p>
------------------	--

### 8.3.1.5 French code of criminal procedure

<b>Reference name</b>	<b>French Code of Criminal Procedure - (art. 60-1, 77-1-1, 93-3)</b>
<b>Original language</b>	French
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	Unauthorized translation
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems

<b>Geographical Scope</b>	France
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Access to images by law enforcement agencies
<b>Additional information</b>	
<b>Description</b>	Access to images is limited to activities of judicial police for the purposes of investigation of crimes and offences sentenced by imprisonment.
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, authorized disclosure
<b>Stage</b>	Design, development, operation
<b>Keywords</b>	
<b>Guidelines</b>	Elements of the system with access to data must be related to the stereotype «control_access». This element restricts access to the elements that can access data.
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Obligation to transmit evidence to law enforcement authorities
<b>Additional information</b>	
<b>Description</b>	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.
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, authorized disclosure
<b>Stage</b>	Operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

### 8.3.1.6 French Data Protection Act (Act n°78-17 of 6 January 1978)

<b>Reference name</b>	<b>French Data Protection Act (Act n°78-17 of 6 January 1978)</b>
<b>Original language</b>	French



<b>Abstract</b>	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.
<b>Link to source</b>	
<b>Link to translation</b>	Unofficial translation
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	France
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	legitimate ground for processing personal data
<b>Additional information</b>	
<b>Description</b>	<p>The processing of personal data must have received the consent of the data subject or must meet one of the following conditions:</p> <p>1° compliance with any legal obligation to which the data controller is subject;</p> <p>2° the protection of the data subject's life;</p> <p>3° the performance of a public service mission entrusted to the data controller or the data recipient;</p> <p>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;</p> <p>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.</p> <p>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.</p> <p>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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	legal basis, data subject's rights accountability
<b>Stage</b>	All
<b>Keywords</b>	

<b>Guidelines</b>	
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Accountability: Data protection officer
<b>Additional information</b>	
<b>Description</b>	<p>A data controller may appoint appointed 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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, accountability transparency
<b>Stage</b>	All
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Security
<b>Additional information</b>	
<b>Description</b>	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-authorised third parties (Art. 34).
<b>Category</b>	Legal
<b>SALT Topics</b>	Proportionality, further use limitation, accountability, transparency
<b>Stage</b>	Operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Entities competent to create forensic systems
<b>Additional information</b>	
<b>Description</b>	Processing of personal data relating to offences, convictions and security measures may be

	<p>put in place only by (art. 9):</p> <p>1°the courts, public authorities and legal entities that manage public services, within the framework of their legal remit;</p> <p>2°the representatives of the law for the strict needs of the exercise of the functions granted to them by the law;</p> <p>3° [Provisions considered contrary to the Constitution by decision No. 2004-499 DC of 29 July 2004 of the Constitutional Court];</p> <p>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.</p> <p>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)</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Proportionality, further use limitation, accountability, transparency
<b>Stage</b>	All stages
<b>Keywords</b>	
<b>Guidelines</b>	Elements of the system with access to personal data must be related to the stereotype «control_access». In order to determine whether the data accessed is personal or not, personal data elements will be associated to the stereotype «personal_data».
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Authorisation
<b>Additional information</b>	
<b>Description</b>	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)
<b>Category</b>	Legal
<b>SALT Topics</b>	further use limitation, accountability, transparency
<b>Stage</b>	Concept, operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Data subject rights
<b>Additional information</b>	
<b>Description</b>	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.

<b>Category</b>	Legal
<b>SALT Topics</b>	accountability, transparency, data subject rights
<b>Stage</b>	
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	-

### **8.3.1.7 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 enforcements 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.

<b>Reference name</b>	<b>Logs and audit tools about operator actions for enhanced accountability</b>
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	

<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Legal basis for the data processing activity
<b>Additional information</b>	Article 4
<b>Description</b>	<p>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):</p> <p>(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 (d) For the prevention of an immediate and serious threat to public security.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Fairness, legal basis, proportionality
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Access to third parties video surveillance systems
<b>Additional information</b>	Article 4a
<b>Description</b>	<p>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)</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Fairness, legal basis, proportionality
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	

<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Access to third parties video surveillance systems, request for access
<b>Additional information</b>	Article 4a 1c
<b>Description</b>	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
<b>Category</b>	Legal
<b>SALT Topics</b>	legal basis
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Access to third parties video surveillance systems data
<b>Additional information</b>	Article 4
<b>Description</b>	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
<b>Category</b>	Legal
<b>SALT Topics</b>	legal basis, fairness, proportionality
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Data retention, deletion
<b>Additional information</b>	Article 4
<b>Description</b>	Personal data should be deleted by law enforcement authorities when they are no longer necessary for the purposes for which they were processed.
<b>Category</b>	Legal
<b>SALT Topics</b>	Data retention
<b>Stage</b>	Concept, design, operation
<b>Keywords</b>	
<b>Guidelines</b>	Elements of the system with access to personal data must be related to the stereotypes «control_access» and «delete». Thanks to the first stereotype, the system places a control access to identify law enforcement authorities. On the other hand, the second stereotype provides a deletion mechanism, thus authorised users who succeeded the control access (law enforcement authorities) have a mechanism to delete personal data when required. In order to determine whether the data accessed is personal or not, personal data elements will be associated to the stereotype «personal_data».
<b>OCL Rules</b>	

<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Data retention, deletion, accountability, data quality
<b>Additional information</b>	Article 4
<b>Description</b>	<p>Law enforcement authorities should put mechanisms in place to ensure that time limits are established for the erasure of personal data. (art. 4b)</p> <p>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)</p> <p>Procedural mechanisms should be established to ensure that those time-limits or the periodic reviews intervals are observed. (art. 4b)</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Data retention
<b>Stage</b>	Concept, design, operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Categorization of data, data quality
<b>Additional information</b>	Article 5.1
<b>Description</b>	<p>Data controllers should make a clear distinction between the following categories of data subjects:</p> <p>(a) Persons with regard to whom there are reasonable grounds for believing that they have committed or are about to commit a criminal offence</p> <p>(b) Persons convicted of a crime</p> <p>(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</p> <p>(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)</p> <p>(e) other</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, proportionality
<b>Stage</b>	Concept, operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Categorization of data, data quality
<b>Additional information</b>	Article 5
<b>Description</b>	<p>Processing of data of other data subjects than the ones mentioned in art. 5.1 may only be processed:</p> <p>(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</p>

	(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.
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, proportionality
<b>Stage</b>	Concept, operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Accuracy and reliability of personal data, data quality, accuracy
<b>Additional information</b>	Article 6.1
<b>Description</b>	The accuracy and reliability of personal data undergoing processing should be ensured.
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, data quality
<b>Stage</b>	Concept, design
<b>Keywords</b>	
<b>Guidelines</b>	Every system element representing a personal data should be associated to the stereotype «personal_data». The OCL rules will look for such elements and will include them into the automatically generated information report. In this way, a user who reads this report will exactly know what to check in order to achieve accuracy and reliability of personal data.
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Categorization of data, data quality, accuracy
<b>Additional information</b>	Article 6.2
<b>Description</b>	Personal data based on facts should be distinguished from personal data based on assessments, in accordance with their degree of accuracy and reliability.
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, data quality
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Categorization of data, specific categories of data
<b>Additional information</b>	Article 8
<b>Description</b>	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



	<p>carried out by law enforcement authorities on the basis of a law; or</p> <p>(b) The processing is necessary to protect the vital interests of the data subject or of another person; or</p> <p>(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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, proportionality
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Data sharing, sharing of incorrect data, unlawful sharing
<b>Additional information</b>	Article 8
<b>Description</b>	<p>If it emerges that incorrect data have been transmitted or data have been transmitted unlawfully, the recipient must be notified without delay.</p> <p>The recipient shall be obliged to rectify the data without delay or to erase them in accordance.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis
<b>Stage</b>	
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Data sharing, transmission of personal data to other parties
<b>Additional information</b>	Article 55
<b>Description</b>	<p>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):</p> <p>(a) The transmission complies with Union or national law; and</p> <p>(b) The recipient is established in a Member State of the European Union; and</p> <p>(c) No legitimate specific interests of the data subject prevent transmission; and</p> <p>(d) The transmission is necessary in a specific case for the controller transmitting the personal data for:</p> <p>(i) The performance of a task lawfully assigned to it; or</p> <p>(ii) The prevention of an immediate and serious danger to public security; or</p> <p>(iii) The prevention of serious harm to the rights of individuals.</p> <p>The controller shall inform:</p> <ul style="list-style-type: none"> <li>• the recipient of the purpose for which the personal data may exclusively be processed</li> <li>• the supervisory authority of such transmissions</li> </ul>

	<ul style="list-style-type: none"> <li>• The recipient of processing restrictions and ensure that these restrictions are met.</li> </ul>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, accountability, further use limitation
<b>Stage</b>	Concept, design, operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Data sharing, requirement for sharing
<b>Additional information</b>	Article 6.3
<b>Description</b>	Personal data shall not be transmitted without request from a competent authority, in particular data originally held by private parties. (Art. 6.3)
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, accountability, further use limitation
<b>Stage</b>	Concept, design, operation
<b>Keywords</b>	
<b>Guidelines</b>	Elements in charge of data transmission must be associated to the stereotype «data_transmission_process». This element must also be associated to the stereotype «control_access» or related to an element associated with such stereotype (dues ensuring that only competent authority with the appropriate privileges will go through the control access mechanism, and hence been allowed for transmitting data).
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 4f)
<b>Additional information</b>	
<b>Description</b>	<p>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.</p> <p>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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, accountability, purpose specification
<b>Stage</b>	Concept, design, operation
<b>Keywords</b>	
<b>Guidelines</b>	An OCL rule to move this information into the information report, so controllers can read it and be aware of their responsibilities regarding to personal data.
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 7a 1
<b>Additional information</b>	
<b>Description</b>	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):

	(a) The purpose is strictly necessary and proportionate in a democratic society and required by law for a legitimate, well-defined and specific purpose; (b) The processing is strictly limited to a period not exceeding the time needed for the specific data processing operation.
<b>Category</b>	Legal
<b>SALT Topics</b>	Legal basis, further use limitation, proportionality, purpose specification
<b>Stage</b>	Concept, design, operation
<b>Keywords</b>	
<b>Guidelines</b>	An OCL rule to include this information into the report <i>[there is no way to automatically check that the purpose is proportionate in a democratic society, this affirmation is too wide]</i> . The system design must also include an element associated to the stereotype «autodeletion» to ensure data removal after the expiration date.
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Articles 9 and 10
<b>Additional information</b>	
<b>Description</b>	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.
<b>Category</b>	Legal
<b>SALT Topics</b>	accountability, purpose specification, transparency
<b>Stage</b>	operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 31 2c) rights of data subjects, contact with the DPO
<b>Additional information</b>	
<b>Description</b>	Data subjects have the right to contact the data protection officer on all issues related to the processing of his or her personal data.
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	Operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)

<b>Name</b>	Article 18
<b>Additional information</b>	Accountability, demonstration of compliance
<b>Description</b>	<p>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)</p> <p>This obligation includes:</p> <p>(a) Keeping the documentation referred to in Article 23 [link to article or reference about art. 23];</p> <p>(a) Performing a data protection impact assessment pursuant to Article 25a [link to article or reference about art. 25a]</p> <p>(b) Complying with the requirements for prior consultation pursuant to Article 26 [link to article or reference about art. 26]</p> <p>(c) Implementing the data security requirements laid down in Article 27 [link to article or reference about art. 27]</p> <p>(d) Designating a data protection officer pursuant to Article 30; [link to article or reference about art. 30]</p> <p>(e) Drawing up and implementing specific safeguards in respect of the treatment of personal data relating to children, where appropriate</p> <p>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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	Concept, design, Operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 23
<b>Additional information</b>	Accountability, documentation
<b>Description</b>	<p>Each controller and processor should maintain documentation of all processing systems and procedures under their responsibility.</p> <p>The documentation shall contain at least the following information:</p> <p>(a) The name and contact details of the controller, or any joint controller or processor;</p> <p>(aa) A legally binding agreement, where there are joint controllers; a list of processors and activities carried out by processors;</p> <p>(b) The purposes of the processing;</p> <p>(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;</p> <p>(bb) A description of the category or categories of data subjects and of the data or categories of data relating to them</p> <p>(c) The recipients or categories of recipients of the personal data;</p> <p>(ca) Where applicable, information about the existence of profiling, of measures based on profiling, and of mechanisms to object to profiling;</p> <p>(cb) Intelligible information about the logic involved in any automated processing;</p> <p>(d) Transfers of data to a third country or an international organisation, including the</p>

	<p>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</p> <p>Articles 35 or 36 of this Directive;</p> <p>(da) The time limits for erasure of the different categories of data;</p> <p>(db) The results of the verifications of the measures referred to in Article 18(1);</p> <p>(dc) An indication of the legal basis of the processing operation for which the data are intended.</p> <p>The controller and the processor shall make all documentation available, on request, to the supervisory authority.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 24
<b>Additional information</b>	Accountability, keeping of records
<b>Description</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• the purpose,</li> <li>• date and time of such operations,</li> <li>• as far as possible the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such data</li> </ul> <p>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.</p> <p>The controller and the processor shall make the records available, on request, to the supervisory authority..</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Transparency, accountability
<b>Stage</b>	Concept, design, operation
<b>Keywords</b>	Records, log, audit
<b>Guidelines</b>	<p>The stereotypes «collection_process», «alteration_process», «consultation_process», «disclosure_process», «combination_process» and «erasure_process» will be associated to those design elements intended for collection, alteration, consultation, disclosure, combination and erasure, respectively. These elements (in case they appear in the system design) will also be associated to the stereotypes «produce_log_entry» and «control_access», or will be related to another element (or elements) with the stereotypes «produce_log_entry» and «control_access». This ensures that only data protection officers and data protection authorities will have the privileges to access the records.</p>
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 30

<b>Additional information</b>	Accountability: data protection officer
<b>Description</b>	<p>The controller or the processor should designate a data protection officer.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability
<b>Stage</b>	Operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 25
<b>Additional information</b>	Accountability: cooperation with supervisory authority sharing access to system
<b>Description</b>	<p>The controller and the processor shall cooperate, on request, with the supervisory authority in the performance of its duties, in particular:</p> <ul style="list-style-type: none"> <li>• by providing access to all personal data and to all information necessary for the performance of its supervisory duties,</li> <li>• 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.</li> </ul> <p>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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, authorized disclosure
<b>Stage</b>	
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 19.1
<b>Additional information</b>	Data protection by design

<b>Description</b>	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.
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 21
<b>Additional information</b>	Subcontracting (processor)
<b>Description</b>	<p>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.</p> <p>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</p> <ul style="list-style-type: none"> <li>(a) act only on instructions from the controller;</li> <li>(b) Employ only staffs who has agreed to be bound by an obligation of confidentiality or are under a statutory obligation of confidentiality;</li> <li>(c) Take all required measures pursuant to Article 27 [link to article or SALT reference];</li> <li>(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;</li> <li>(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];</li> <li>(f) Assist the controller in ensuring compliance with the obligations pursuant to Articles 25a to 29 [link to article or SALT reference];</li> <li>(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;</li> <li>(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;</li> <li>(i) Take into account the principle of data protection by design and default</li> </ul>

	The controller and the processor shall document in writing the controller's instructions and the processor's obligations.
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 19.1
<b>Additional information</b>	Data protection by design
<b>Description</b>	<p>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. 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.</p> <p>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</p> <ul style="list-style-type: none"> <li>(a) act only on instructions from the controller;</li> <li>(b) Employ only staffs who has agreed to be bound by an obligation of confidentiality or are under a statutory obligation of confidentiality;</li> <li>(c) Take all required measures pursuant to Article 27 [link to article or SALT reference];</li> <li>(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;</li> <li>(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];</li> <li>(f) Assist the controller in ensuring compliance with the obligations pursuant to Articles 25a to 29 [link to article or SALT reference];</li> <li>(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;</li> <li>(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;</li> </ul>



	(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
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 19.2
<b>Additional information</b>	Data protection by default
<b>Description</b>	<p>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. 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.</p> <p>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</p> <ul style="list-style-type: none"> <li>(a) act only on instructions from the controller;</li> <li>(b) Employ only staffs who has agreed to be bound by an obligation of confidentiality or are under a statutory obligation of confidentiality;</li> <li>(c) Take all required measures pursuant to Article 27 [link to article or SALT reference];</li> <li>(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;</li> <li>(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];</li> <li>(f) Assist the controller in ensuring compliance with the obligations pursuant to Articles 25a to 29 [link to article or SALT reference];</li> <li>(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;</li> <li>(h) Make available to the controller and the supervisory authority all the information</li> </ul>

	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 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)
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency, data minimization, data retention
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 27
<b>Additional information</b>	Security
<b>Description</b>	<p>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</p> <p>In respect of automated data processing, the controller or processor, following an evaluation of the risks, should implement measures designed to:</p> <p>(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);</p> <p>(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);</p> <p>(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);</p> <p>(d) prevent the use of automated data processing systems by unauthorised persons using data communication equipment (user control);</p> <p>(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)</p> <p>(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);</p> <p>(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)</p> <p>(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);</p> <p>(i) ensure that installed systems may, in case of interruption, be restored (recovery);</p> <p>(j)(j) ensure that the functions of the system perform, that the appearance of faults in</p> <p>(k) the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity);</p> <p>(l)(ja) ensure that in case of sensitive</p> <p>(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</p>

	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.
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency, data security
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

### 8.3.1.8 General data protection regulation

<b>Reference name</b>	EU data Protection Regulation Proposal (not approved yet)
<b>Original language</b>	English
<b>Abstract</b>	All processing of personal data except certain specific processing
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	European Union
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 23
<b>Additional information</b>	Accountability: general obligations
<b>Description</b>	<p>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.</p> <p>Policies: Should be documented and at minimum include information about the following</p>

	<p>items:</p> <ul style="list-style-type: none"> <li>• collection, use and disclosure of personal information, including requirements for consent and notification;</li> <li>• procedure to access to and correction of personal information;</li> <li>• retention and disposal of personal information;</li> <li>• 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.</li> <li>•</li> </ul> <p>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.</p> <p>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.</p>
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency, data subject's rights
<b>Stage</b>	Concept
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 32a, main part
<b>Additional information</b>	Data protection impact assessment
<b>Description</b>	<p>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.</p> <p>It is mandatory in the following cases:</p> <ul style="list-style-type: none"> <li>• processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;</li> </ul>

- 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.
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	Concept, operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Article 32a, periodic reviews
<b>Additional information</b>	Data protection Impact assessment, periodic reviews
<b>Description</b>	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.
<b>Category</b>	Legal
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	Concept, operation
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

### **8.3.1.9 Criminal Procedure Code (Strafprozeßordnung, StPO) on Seizure, Interception of Telecommunications, Computer-assisted Search, Use of Technical Devices, Use of Undercover Investigators and Search**

Field	Type	Description
<b>Reference name</b>	Mandatory	<i>Criminal Procedure Code (Strafprozeßordnung, StPO) on Seizure, Interception of Telecommunications, Computer-assisted Search, Use of Technical Devices, Use of Undercover Investigators and Search</i>
<b>Original language</b>	Mandatory	German
<b>Abstract</b>	Optional	Sections in Austrian criminal law that is relevant to the use of video surveillance data for criminal investigation.
<b>Link to source</b>	Optional	<a href="https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&amp;Gesetzesnummer=10002326">https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&amp;Gesetzesnummer=10002326</a>
<b>Link to translation</b>	Optional	<a href="http://www.iuscomp.org/gla/statutes/StPO.htm">http://www.iuscomp.org/gla/statutes/StPO.htm</a>
<b>Official translation</b>	Optional	[Ye] <a href="https://www.ris.bka.gv.at/defaultEn.aspx">https://www.ris.bka.gv.at/defaultEn.aspx</a>
<b>System type</b>	Mandatory	<i>Video surveillance systems</i>

<b>Geographical Scope</b>	Mandatory	Within Austria.
<b>Context</b>	Optional	<i>Law related to use video surveillance data for criminal investigation</i>
<b>Version</b>	Mandatory	v0.1
<b>Keywords</b>	Optional	
<b>Creator</b>	Automatic	Zhendong Ma
<b>Last update</b>	Automatic	<i>June</i>
<i>List of concerns (privacy and accountability related concerns for surveillance systems)</i>		
<b>Concern ID</b>	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
<b>Name</b>	Mandatory	Austrian criminal procedure code
<b>Additional information</b>	Optional	
<b>Description</b>	Mandatory	<p>Basically all objects (which apply to video surveillance footage) should be securely obtained and kept for evidence (including sound, image, or other recorded data) during criminal investigation. The retention ends, as soon as the purpose is fulfilled. All measures should take section 5 of StPO (i.e. for the duration of joinder the proceedings shall be governed by the criminal case within the jurisdiction of the court of higher rank.) into consideration. The measures should be only used for defined purpose and should be necessary, in order to fulfill the defined objective.</p> <p>The police is not allowed to take privacy invading data for minor crimes that either don't matter that much or can be solved without the data just as easy. The measures taken must be in proportion to the gravity of the criminal act.</p>
<b>Category</b>	Mandatory	Legal
<b>SALT Topics</b>	Mandatory	Legal framework for data usage
<b>Stage</b>	Optional	<p>Stage or stages of the SALT Process in which this concern applies.</p> <p>These are the stages defined and their goals:</p> <ul style="list-style-type: none"> <li>• <b>concept</b> (intention): selection of the most suitable solution to solve the stakeholder's problem;</li> <li>• <b>design</b>: elaboration of the system design according to the different requirements;</li> <li>• <b>development</b>: implementation of the system based on the defined specification;</li> <li>• <b>deployment</b>: set up the system in the stakeholder's environment;</li> <li>• <b>operation &amp; maintenance</b>: use the system and ensure its correct functioning to satisfy stakeholder's needs;</li> </ul>
<b>Keywords</b>	Optional	Criminal investigation, evidence
<b>Guidelines</b>	Optional	The criminal law permits the use of video surveillance footage as evidence in criminal investigation. However, the usage must not beyond the defined purpose.
<b>OCL Rules</b>	Optional	

## 8.3.2 Socio-Ethical references for the video-surveillance use-case

### 8.3.2.1 List of Socio-Ethical artifacts

The table below lists the Socio-Ethical artifacts that are proposed to illustrate the development of the video-surveillance use-case. Many other system could be proposed.

References description. Fields	References descriptions
<b>Reference name</b>	<b>2008 CNIL study : French people and videosurveillance”</b>
<b>System type</b>	All video-surveillance systems
<b>Geographical scope</b>	Worldwide
<b>Reference name</b>	<b>“Surveillance ethics from the Internet Encyclopedia of Philosophy”</b>
<b>System type</b>	All surveillance systems
<b>Geographical scope</b>	Worldwide
<b>Reference name</b>	<b>“video-surveillance in retail places: ethical perspective ”</b>
<b>System type</b>	All surveillance systems
<b>Geographical scope</b>	Worldwide

### 8.3.2.2 2008 CNIL study: French people and video-surveillance

Reference name	2008 French survey on video-surveillance
<b>Original language</b>	French
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	France, Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	



<b>Creator</b>	Thales																
<b>Last update</b>	20/12/2014																
<i>List of concerns</i>																	
<b>Concern ID</b>	<b>TBD (SFMT)</b>																
<b>Name</b>	Perception of efficiency of cameras																
<b>Additional information</b>																	
<b>Description</b>	<p>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?”</p> <table border="1"> <caption>Survey Results for Concern ID TBD (SFMT)</caption> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>yes, completely</td> <td>27%</td> </tr> <tr> <td>yes, in a way</td> <td>38%</td> </tr> <tr> <td>Not really</td> <td>19%</td> </tr> <tr> <td>not at all</td> <td>14%</td> </tr> <tr> <td>NSP</td> <td>2%</td> </tr> <tr> <td><b>S/ T « OUI »</b></td> <td><b>65%</b></td> </tr> <tr> <td><b>S/ T « NON »</b></td> <td><b>33%</b></td> </tr> </tbody> </table>	Response	Percentage	yes, completely	27%	yes, in a way	38%	Not really	19%	not at all	14%	NSP	2%	<b>S/ T « OUI »</b>	<b>65%</b>	<b>S/ T « NON »</b>	<b>33%</b>
Response	Percentage																
yes, completely	27%																
yes, in a way	38%																
Not really	19%																
not at all	14%																
NSP	2%																
<b>S/ T « OUI »</b>	<b>65%</b>																
<b>S/ T « NON »</b>	<b>33%</b>																
<b>Category</b>	Socio-Ethical																
<b>SALT Topics</b>	All																
<b>Stage</b>	Intention																
<b>Keywords</b>																	
<b>Guidelines</b>																	
<b>OCL Rules</b>																	
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>																
<b>Name</b>	importance of controls on video-surveillance cameras placed in public space																
<b>Additional information</b>																	
<b>Description</b>	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”?																

	<p><b>S/ T « IMPORTANT »</b> 79%</p> <p><b>S/ T « PAS IMPORTANT »</b> 17%</p> <p>47% 32% 10% 7% 4%</p> <p>very important rather important not really important not at all important NSP</p>
<b>Category</b>	Socio-Ethical
<b>SALT Topics</b>	All
<b>Stage</b>	Intention
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	General opinion about video-surveillance
<b>Additional information</b>	
<b>Description</b>	<p>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?”</p> <p><b>S/ T « FAVORABLE »</b> 71%</p> <p><b>S/ T « DEFAVORABLE »</b> 28%</p> <p>50% 21% 15% 13% 1%</p> <p>strongly agree rather agree rather disagree strongly disagree NSP</p>
<b>Category</b>	Socio-Ethical
<b>SALT Topics</b>	All

<b>Stage</b>	Intention
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

### 8.3.2.3 *Surveillance ethics from the internet encyclopedia of philosophy*

<b>Reference name</b>	<b>3.2.3 Surveillance ethics from the internet encyclopedia of philosophy (abstract)</b>
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	All
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	Data protection, European legal framework
<b>Creator</b>	Thales
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Ethics of surveillance from a philosophical perspective
<b>Additional information</b>	
<b>Description</b>	<p>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.</p> <p>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?</p> <p>This article provides a brief overview of the history of surveillance ethics, beginning with</p>

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

	<p>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.</p> <p>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.</p> <p>2. Recent History</p> <p>While Bentham/Foucault and Orwell successfully raised questions about the value and harms of surveillance, these had limited impact in many philosophy departments [...]</p>
<b>Category</b>	Socio-Ethical
<b>SALT Topics</b>	
<b>Stage</b>	
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	importance of controls on video-surveillance cameras placed in public space
<b>Additional information</b>	
<b>Description</b>	
<b>Category</b>	Technical
<b>SALT Topics</b>	
<b>Stage</b>	
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

#### 8.3.2.4 Video-surveillance in retail places: ethical perspective

<b>Reference name</b>	"video-surveillance research in retailing: ethical issues"
<b>Original language</b>	English
<b>Abstract</b>	

<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	Thales
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Abstract
<b>Additional information</b>	
<b>Description</b>	<p>Abstract:</p> <p>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.</p>
<b>Category</b>	Socio-ethical
<b>SALT Topics</b>	All
<b>Stage</b>	intention
<b>Keywords</b>	
<b>Guidelines</b>	.
<b>OCL Rules</b>	

### 8.3.3 Technical references for the video-surveillance use-case

#### 8.3.3.1 Technical references list

References description. Fields	References descriptions	Technical descriptions	Privacy risks	PET
<b>Reference name</b>	<b>CNIL Security Guide</b>			
<b>System type</b>	All			
<b>Geographical scope</b>	France	*	**	**
<b>Reference name</b>	<b>Denial of service risk IT attack on camera</b>			
<b>System type</b>	All video-surveillance systems	**	***	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Encryption and signature of video data: principles and benefits</b>			
<b>System type</b>	All video-surveillance systems	**	*	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Logical access control to video-surveillance systems</b>			
<b>System type</b>	All video-surveillance systems	*	**	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Capabilities of google-glass cameras</b>			
<b>System type</b>	All video-surveillance systems	**	*	*
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Logs and audit tools about operator actions for enhanced accountability</b>			
<b>System type</b>	All surveillance systems	**	*	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Resolution of video images and recognition performances</b>			
<b>System type</b>	All video-surveillance systems	***	***	***
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Scalability of video analytics</b>			
<b>System type</b>	video-surveillance systems			
<b>Geographical</b>	Worldwide	***		

<b>scope</b>				
<b>Reference name</b>	<b>Detection quality of video analytics</b>	***		
<b>System type</b>	video-surveillance systems			
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Privacy risks management</b>	*	**	*
<b>System type</b>	video-surveillance systems			
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Architecture pattern: access control for video archive search</b>	***	*	**
<b>System type</b>	All video-surveillance systems			
<b>Geographical scope</b>	Worldwide			
<b>Reference name</b>	<b>Interoperability of authentication and identity management</b>	***	*	*
<b>System type</b>	All surveillance systems			
<b>Geographical scope</b>	Worldwide			

### 8.3.3.2 CNIL security guide

<b>Reference name</b>	<b>CNIL security guide</b>
<b>Original language</b>	French and English (2 versions provided by the CNIL)
<b>Abstract</b>	
<b>Link to source</b>	<a href="http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf">http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf</a>
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	All systems
<b>Geographical Scope</b>	France
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	NAMUR
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Security: authorization management



<b>Additional information</b>	
<b>Description</b>	<p>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:</p> <ul style="list-style-type: none"> <li>- providing a unique identifier to each user, in association with authentication means: an authentication method;</li> <li>- applying prior access controls to data for each category of users: an authorisation management.</li> </ul>
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security, authorized disclosure
<b>Stage</b>	Design, development
<b>Keywords</b>	
<b>Guidelines</b>	System users (who can be distinguished thanks to the stereotype «system_user») must be related to another element associated to the stereotype «control_access».
<b>OCL Rules</b>	<p>CNIL.1  context System_user inv CNIL.1  not self.access.ocllsUndefined()</p>
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Security: keeping records and documentation of data processing operations
<b>Additional information</b>	<p>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).</p> <p>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.</p>
<b>Description</b>	
<b>Category</b>	Technical
<b>SALT Topics</b>	Fairness, legal basis, further use limitation, accountability, data security
<b>Stage</b>	Design, development, operation
<b>Keywords</b>	
<b>Guidelines</b>	Elements with the stereotype «system_user» must be related to at least one element with the stereotype «produce_log_entry».
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Security: storage
<b>Additional information</b>	

<b>Description</b>	<p>The Privacy Management Program/internal privacy policy should indicate practices and policies which would allow ensuring the secure storage of collected personal data.</p> <p>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.</p> <p>To protect against leakage of personal data, the video footages should be stored in an encrypted form in the video databases.</p> <p>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.</p>
<b>Category</b>	Legal, technical
<b>SALT Topics</b>	Data security, authorized disclosure
<b>Stage</b>	Design, development, operation
<b>Keywords</b>	
<b>Guidelines</b>	<p>Elements with the stereotype «personal_data» must also be associated to the stereotype «encrypted_data». They also have to be associated to the stereotype «control_access» or have a relation with another element associated to the stereotype «control_access».</p> <p>The system model must also contain at least one element associated to the stereotype «autodeletion».</p>
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Security: incident management
<b>Additional information</b>	
<b>Description</b>	<p>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.</p>
<b>Category</b>	Legal, technical
<b>SALT Topics</b>	
<b>Stage</b>	Concept, design
<b>Keywords</b>	
<b>Guidelines</b>	I think this concern relates just to the concept stage.
<b>OCL Rules</b>	-

### 8.3.3.3 Denial of service risk IT attack on a camera

<b>Reference name</b>	<b>Denial of service IT attack on a camera: risks and possible remediation</b>
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	

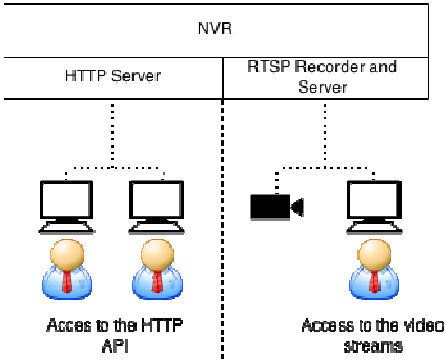
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	Thales
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	Description of risk
<b>Additional information</b>	
<b>Description</b>	<p>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.</p> <p>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).</p>
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security
<b>Stage</b>	Design, development
<b>Keywords</b>	Hacker, IT attack
<b>Guidelines</b>	All elements representing a camera will be associated to the stereotype «camera» with the boolean attribute «protection_mode» set to true.
<b>OCL Rules</b>	
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	possible remediation to DoS attack on a camera: temporization
<b>Additional information</b>	
<b>Description</b>	A temporization between the submission of a request to the camera on the management port and the answer to the request is implemented.
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security
<b>Stage</b>	Design, development
<b>Keywords</b>	Hacker, IT attack, protection
<b>Guidelines</b>	All elements representing a camera will be associated to the stereotype «camera» with the boolean attribute «temporization_method» set to true.
<b>OCL Rules</b>	camera: delay of answers on management port activated (This is not a valid OCL rule).
<b>Concern ID</b>	TBD (from SALT tools)

<b>Name</b>	possible remediation to DoS attack on a camera: network hardening using 802.1X network-level authentication
<b>Additional information</b>	
<b>Description</b>	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.
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security
<b>Stage</b>	Design, development
<b>Keywords</b>	Hacker, IT attack, protection
<b>Guidelines</b>	All elements representing a camera and a switch will be associated to the stereotypes «camera» and «switch», respectively. These stereotypes will have their boolean attributes «802.1X_authentication» set to true.
<b>OCL Rules</b>	

#### 8.3.3.4 Encryption and signature of video data: principles and benefits

<b>Reference name</b>	Encryption and signature of video data: principles, technologies and benefits
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	SSL, HTTPS, encryption
<b>Creator</b>	Thales
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	main principles and benefits of video data encryption
<b>Additional information</b>	
<b>Description</b>	The encryption of the video streams, even if not simple to perform, brings many gains: it

	<p>allows preventing the unexpected, unauthorized viewing of the video-stream issued from the video-surveillance camera to happen.</p> <p>The signature of streams, and especially of exports, enable to guarantee data integrity, by checking that no modification of data occurred.</p> <p>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.</p> <p>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).</p> <p>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 camera because of a crisis situation). Also, some states may limit the type and/or strength and/or type of allowed encryption.</p> <p>2 main categories of encryption can be implemented: the encryption within the streams, and the encryption at network level.</p>
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security
<b>Stage</b>	Design, development
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	-
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Network level encryption rule
<b>Additional information</b>	
<b>Description</b>	The encryption performed at the network level is realized using standard network security processes such as SSL (the well-known secured version of the HTTP protocol, HTTPS, is based on this process) or VPN (Virtual Private Network). It raises the advantage of being well known about the exact level of security provided (level of difficulty to break the encryption), but is expensive to put in place and also to maintain because of needed regular updates of the system.
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security
<b>Stage</b>	Design, development
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (from SALT tools)
<b>Name</b>	Within-stream encryption rule

<b>Additional information</b>	
<b>Description</b>	The stream-level encryption is most often a proprietary software capability, performing in-stream encryption one side, and decryption the other side. The advantage is that it may be lighter to handle than a more common network-level encryption capability (nevertheless not always true). The drawback is the difficulty to assess to actual level of hardening of the data performed.
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security,
<b>Stage</b>	Design, development
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	
<b>Concern ID</b>	TBD (from SALT tools)
<b>Name</b>	Network interfaces binding
<b>Additional information</b>	
<b>Description</b>	<p>Adding security / flexibility to the way the NVR is integrated in systems can be done by using a VPN and binding a server to the virtual interface created by the VPN, one can easily add another layer of security to the HTTP API or the RTSP server.</p> <p>- The functionalities can be segmented between different networks, either physical (different network cards) or logical (VPN), preventing unauthorized access to video streams. Such a separation is illustrated in Fig. 2.</p>  <p>The diagram illustrates the NVR architecture. At the top, a box labeled 'NVR' is divided into two sections: 'HTTP Server' on the left and 'RTSP Recorder and Server' on the right. Below the 'HTTP Server' section, two laptop icons are shown, with a person icon below them, labeled 'Access to the HTTP API'. Below the 'RTSP Recorder and Server' section, a camera icon and a laptop icon are shown, with a person icon below them, labeled 'Access to the video streams'. A vertical dashed line separates the two sections, indicating logical segmentation.</p>
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security
<b>Stage</b>	Design, development
<b>Keywords</b>	
<b>Guidelines</b>	<p>The system design must have at least:</p> <ul style="list-style-type: none"> <li>• One element with the stereotype «network_card» and one element with the stereotype «VPN».</li> <li>• Two elements with the stereotype «network_card».</li> <li>• Two elements with the stereotype «VPN».</li> </ul>
<b>OCL Rules</b>	<p>Encryption.1  context Class inv Encryption.1  (ParisProfile::VideoSurveillance::Network_card::allInstances()-&gt;size())&gt;=1 and  ParisProfile::VideoSurveillance::VPN::allInstances()-&gt;size())&gt;=1) or  (ParisProfile::VideoSurveillance::Network_card::allInstances()-&gt;size())&gt;1) or</p>

	(ParisProfile::VideoSurveillance::VPN::allInstances()->size())>1)
<b>Concern ID</b>	TBD (from SALT tools)
<b>Name</b>	Signature of video exports
<b>Additional information</b>	
<b>Description</b>	Encrypted signature of video exports enables to check, using a dedicated software, that the video has not been modified from its export.
<b>Category</b>	Technical
<b>SALT Topics</b>	Data security, data quality
<b>Stage</b>	Design, development
<b>Keywords</b>	
<b>Guidelines</b>	System elements associated to the stereotype «data_transmission_process» (a video export is a kind of data transmission) must have the corresponding boolean attribute «encrypted_signature» set to true.
<b>OCL Rules</b>	Encryption.2 context Data_transmission_process inv Encryption.2 self.encrypted_signature=true

### 8.3.3.5 Logical access controls to video-surveillance systems

<b>Reference name</b>	Access to images by law enforcement authorities in Belgium
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	RBAC, access control
<b>Creator</b>	AIT
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Role based Access Control
<b>Additional</b>	

<b>information</b>	
<b>Description</b>	<p>Role Based Access Control</p> <p>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.</p>
<b>Category</b>	Technical
<b>SALT Topics</b>	Authorized disclosure, accountability, data security
<b>Stage</b>	Design, development
<b>Keywords</b>	RBAC, access control
<b>Guidelines</b>	Elements with the stereotype «system_user» must be related to at least one element with the stereotype «control_access».
<b>OCL Rules</b>	
<b>Concern ID</b>	<b>TBD (from SALT tools)</b>
<b>Name</b>	Attribute-based access control
<b>Additional information</b>	
<b>Description</b>	<p>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).</p> <p>Every permission record - policy entry - has several attributes:</p> <ul style="list-style-type: none"> <li>• users (subject)</li> <li>• validity (environment)</li> <li>• permissions (groups of attributes)</li> <li>• cameras &amp; their time frame (resource)</li> <li>• algorithms (action)</li> </ul> <p>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.</p>
<b>Category</b>	Technical
<b>SALT Topics</b>	Authorized disclosure, accountability, data security
<b>Stage</b>	Design, development
<b>Keywords</b>	access control
<b>Guidelines</b>	<p>Elements with the stereotype «system_user» must be related to at least one element with the stereotype «abac_access_control». All attributes from the stereotype «abac_access_control» must be set to a specific value (not empty). List of (text based) attributes:</p> <ul style="list-style-type: none"> <li>• «subject»</li> <li>• «environment»</li> <li>• «permissions»</li> <li>• «resources»</li> </ul>



	• «algorithms»
<b>OCL Rules</b>	

### 8.3.3.6 Capabilities of Google-Glass cameras

<b>Reference name</b>	technical capabilities of "Google glass" cameras
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	Wearable devices, mobile devices
<b>Creator</b>	Thales
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Description of google glass and their use
<b>Additional information</b>	
<b>Description</b>	<p>The Google glasses are glasses equipped with miniaturized devices that enable their wearer:</p> <ul style="list-style-type: none"> <li>• To see video information in his field of vision (including augmented reality, meaning information contextualized from information such as position, ongoing task...)</li> <li>• Thanks to an embedded camera and micro, to film and to send video and audio streams to external devices using a WIFI connection</li> </ul>
<b>Category</b>	technical
<b>SALT Topics</b>	Data minimization, accountability, authorized disclosure
<b>Stage</b>	Intention, design
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	-

Concern ID	TBD (from SALT tools)
<b>Name</b>	Possible privacy harms and remediation
<b>Additional information</b>	
<b>Description</b>	<p>The Google glass devices enables privacy harms by allowing very discrete video capture, sending, and recording.</p> <p>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.</p>
<b>Category</b>	Technical
<b>SALT Topics</b>	Data minimization, accountability, authorized disclosure
<b>Stage</b>	design, development
<b>Keywords</b>	
<b>Guidelines</b>	System elements representing Google glasses must be associated to the stereotype «google_glass». This stereotype has a boolean attribute «prevent_transmission», which can be set to true or false, depending on the system context.
<b>OCL Rules</b>	

### 8.3.3.7 Operators actions logging

<b>Reference name</b>	Logs and audit tools about operator actions for enhanced accountability
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	Accountability, logging, operators actions, auditability
<b>Creator</b>	Thales
<b>Last update</b>	20/12/2014
<i>List of concerns</i>	
<b>Concern ID</b>	TBD (SFMT)
<b>Name</b>	Benefit and methods of operators actions logging

<b>Additional information</b>	
<b>Description</b>	<p>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.</p> <p>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.</p> <p>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.</p>
<b>Category</b>	Technical
<b>SALT Topics</b>	Accountability, transparency
<b>Stage</b>	System elements with the stereotype «system_user» must also have the stereotype «produce_log_entry». If that is not the case, then it has to be related to another system element associated to the stereotype «produce_log_entry».
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

### 8.3.3.8 Resolution of video stream

<b>Reference name</b>	Resolution of video images and recognition performances
<b>Original language</b>	English
<b>Abstract</b>	
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	resolution, balance between security and privacy
<b>Creator</b>	Thales
<b>Last update</b>	20/12/2014

<i>List of concerns</i>	
Concern ID	TBD (SFMT)
<b>Name</b>	Recognition performance versus camera resolution
<b>Additional information</b>	
<b>Description</b>	<p>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).</p> <p>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.</p> <p>An illustration of the strength of the resolution upon image embedded information is shown below (image from a Whitepaper from the MOTOROLA firm ).</p> <p>Figure 16: impact of image resolution upon the potential performance of a video-surveillance system</p> <p>It is generally recognized that 40PPF is the needed resolution for possible face identification, while 80PPF is needed for license plate reading.</p> <p>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 performance is. So the higher the physical resolution is, the higher the security level is, the lower the privacy is.</p> <p>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.</p>
<b>Category</b>	technical
<b>SALT Topics</b>	Data quality, data minimization
<b>Stage</b>	Concept, design
<b>Keywords</b>	<p>System elements representing a camera are associated to the stereotype «camera». This stereotype has several attributes, but this concern refers to two of them: «objective» and «resolution».</p> <ul style="list-style-type: none"> <li>• If «objective» = “face identification”, then «resolution» must be equal or greater than 40.</li> <li>• If «objective» = “license plate”, then «resolution» must be equal or greater than 80.</li> </ul>
<b>Guidelines</b>	<p>VString.1 context Camera inv VString.1 self.objective = 'face identification' implies self.resolution_ppf&gt;39</p> <p>VString.2</p>

	context Camera inv VString.2 self.objective = 'license_plate' implies self.resolution_ppf>79
<b>OCL Rules</b>	

### 8.3.3.9 Saleability of video analytics

<b>Reference name</b>	<b>Saleability of video analytics</b>
<b>Original language</b>	English
<b>Abstract</b>	Independent video sources can be analysed in parallel (scales well) combining multiple sources or adding more analytics to one source is difficult to parallelize (does not scale well)
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	AIT
<b>Last update</b>	19/06/2015
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	
<b>Additional information</b>	
<b>Description</b>	
<b>Category</b>	Technical
<b>SALT Topics</b>	
<b>Stage</b>	Concept, design
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

### 8.3.3.10 Detection Quality of video analytics

<b>Reference name</b>	<b>Detection Quality of video analytics</b>
-----------------------	---

<b>Original language</b>	English
<b>Abstract</b>	No 100% detection (Depending on the used algorithms, type of tasks, source quality, the results quality can vary from good to unusable.) False Alarms vs. missed detections (There is always the trade-off between generating too many false alarms and missing an event/detection.)
<b>Link to source</b>	
<b>Link to translation</b>	
<b>Official translation</b>	
<b>System type</b>	Video-surveillance systems
<b>Geographical Scope</b>	Any
<b>Context</b>	
<b>Version</b>	0.1
<b>Keywords</b>	
<b>Creator</b>	AIT
<b>Last update</b>	16/06/2015
<i>List of concerns</i>	
<b>Concern ID</b>	<b>TBD (SFMT)</b>
<b>Name</b>	
<b>Additional information</b>	
<b>Description</b>	
<b>Category</b>	Technical
<b>SALT Topics</b>	
<b>Stage</b>	Concept, design
<b>Keywords</b>	
<b>Guidelines</b>	
<b>OCL Rules</b>	

### 8.3.3.11 Privacy risk management

Field	Type	Description
<b>Reference name</b>	Mandatory	<i>Privacy risk assessment</i>
<b>Original language</b>	Mandatory	French (Gérer les risques sur les libertés et la vie privée, la méthode")
<b>Abstract</b>	Optional	To ensure data protection within information systems, methods for managing risks are needed. The privacy risk assessment methodology follows the CNIL guide, and consists a analytical approach for improving the management of processing of personal data.

<b>Link to source</b>	Optional	<a href="http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf">http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf</a>
<b>Link to translation</b>	Optional	Link to the source of information translated to English
<b>Official translation</b>	Optional	[ No]
<b>System type</b>	Mandatory	Information systems/ all systems
<b>Geographical Scope</b>	Mandatory	France, but as a methodology, also applicable to other EU states
<b>Context</b>	Optional	
<b>Version</b>	Mandatory	V0.1
<b>Keywords</b>	Optional	Privacy risk, risk management
<b>Creator</b>	Automatic	Zhendong Ma
<b>Last update</b>	Automatic	Date and time of the last reference update ( <i>automatically filled by the SF Tool</i> )
<i>List of concerns (privacy and accountability related concerns for surveillance systems)</i>		
<b>Concern ID</b>	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
<b>Name</b>	Mandatory	Privacy Risk Management
<b>Additional information</b>	Optional	Methodology and approaches for managing risks regarding personal data in information systems.
<b>Description</b>	Mandatory	Privacy risk management methodology is a catalog of measures intended to address risks of processing personal data.
<b>Category</b>	Mandatory	<i>Technical.</i>
<b>SALT Topics</b>	Mandatory	Technical compliance
<b>Stage</b>	Optional	Stage or stages of the SALT Process in which this concern applies. These are the stages defined and their goals: <ul style="list-style-type: none"> <li>• <b>concept</b> (intention): selection of the most suitable solution to solve the stakeholder's problem;</li> <li>• <b>design</b>: elaboration of the system design according to the different requirements;</li> <li>• <b>development</b>: implementation of the system based on the defined specification;</li> <li>• <b>deployment</b>: set up the system in the stakeholder's environment;</li> <li>• <b>operation &amp; maintenance</b>: use the system and ensure its correct functioning to satisfy stakeholder's needs;</li> <li>• <b>retirement</b>: shut down the system in a controlled manner.</li> </ul>
<b>Keywords</b>	Optional	Risk management, privacy risks, compliance,
<b>Guidelines</b>	Optional	The five iterative steps of the risk management approaches <ol style="list-style-type: none"> <li>1. context</li> <li>2. feared events</li> <li>3. threats</li> <li>4. risks</li> <li>5. measures</li> </ol>
<b>OCL Rules</b>	Optional	

**8.3.3.12 Architecture pattern: access control for video archive search**

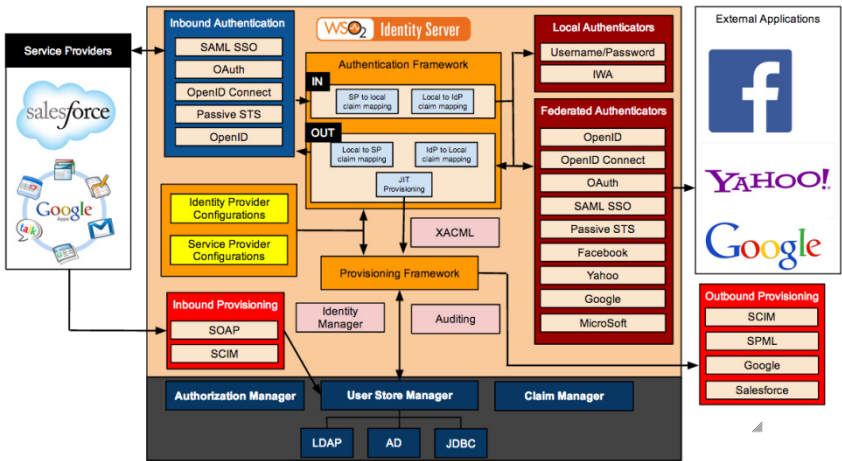
Field	Type	Description
Reference name	Mandatory	Architecture design: access control for video archive search
Original language	Mandatory	English
Abstract	Optional	Access control is one of the technical measures to ensure the privacy of personal data in information systems. It consists of authentication, authorisation and the enforcement of defined privacy policy.
Link to source	Optional	Link to the source of information in the original language
Link to translation	Optional	Link to the source of information translated to English
Official translation	Optional	[No]
System type	Mandatory	Video surveillance systems
Geographical Scope	Mandatory	This architecture pattern is applicable to Austrian legal framework.
Context	Optional	Access control architecture is the technical means to implement policy and procedures, consistent with applicable data protection laws.
Version	Mandatory	v0.1
Keywords	Optional	Access control, authentication, authorization, security controls, policies, procedures
Creator	Automatic	Zhendong Ma
Last update	Automatic	Date and time of the last reference update (automatically filled by the SF Tool)
<i>List of concerns (privacy and accountability related concerns for surveillance systems)</i>		
Concern ID	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
Name	Mandatory	Architecture pattern: access control for video archive search
Additional information	Optional	This architecture pattern can be adopted for information systems that must implement and enforce access control for data protection.
Description	Mandatory	<p>Access control is a security and privacy control that provide selective restriction of access to information.</p>
Category	Mandatory	Technical.



<b>SALT Topics</b>	Mandatory	Technical privacy control
<b>Stage</b>	Optional	<ul style="list-style-type: none"> <li><b>design:</b> elaboration of the system design according to the different requirements;</li> </ul>
<b>Keywords</b>	Optional	Access control, authentication, authorization
<b>Guidelines</b>	Optional	System elements associated to the stereotype «personal_data» and/or «sensitive_data» must also be associated to the stereotype «control_access». If that is not the case, they must be related to another system element associated to the stereotype «control_access».
<b>OCL Rules</b>	Optional	<p>Architecture.1 context Personal_Data inv Architecture.1 not self.access.ocllsUndefined()</p> <p>Architecture.2 context Sensitive_Data inv Architecture.2 not self.access.ocllsUndefined()</p>

### 8.3.3.13 Interoperability of authentication and identity management

Field	Type	Description
<b>Reference name</b>	Mandatory	Interoperability of authentication and identity management
<b>Original language</b>	Mandatory	English
<b>Abstract</b>	Optional	Authentication and identity management (AIM) is the basis for making access control decisions. Authentication is an identity verification process to determine whether users are who they say they are. A user needs to have an account at an identity provider. On UNIX system, users might have an account in an LDAP databased the UNIX host recognize. On Windows, users might have Active Directory account. AIM can be based on different technologies across organizations. Identity accounts might be provided and managed by different parties. Therefore, interoperability is a very important issue.
<b>Link to source</b>	Optional	Link to the source of information in the original language
<b>Link to translation</b>	Optional	Link to the source of information translated to English
<b>Official translation</b>	Optional	[No]
<b>System type</b>	Mandatory	<i>All systems</i>
<b>Geographical Scope</b>	Mandatory	Any
<b>Context</b>	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference ( <i>e.g. specific cases/conditions where the reference is applicable</i> ).
<b>Version</b>	Mandatory	v0.1
<b>Keywords</b>	Optional	Authentication, identity management, interoperability
<b>Creator</b>	Automatic	Zhendong Ma
<b>Last update</b>	Automatic	Date and time of the last reference update ( <i>automatically filled by the SF Tool</i> )
<i>List of concerns (privacy and accountability related concerns for surveillance systems)</i>		
<b>Concern ID</b>	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)

<b>Name</b>	Mandatory	Interoperability of authentication and identity management
<b>Additional information</b>	Optional	Examples to address interoperability of AIM
<b>Description</b>	Mandatory	<p>Authentication and identity management (AIM) is the basis for making access control decisions. Interoperability among different identity providers is important for making access control decision. Existing technologies can leverage multiple identity sources for authentication and identity management. For example, the WSO2 identity server used for PEAC</p>  <p>The diagram illustrates the WSO2 Identity Server architecture. It is divided into several main sections:         <ul style="list-style-type: none"> <li><b>Service Providers:</b> Includes Salesforce and Google.</li> <li><b>Inbound Authentication:</b> Lists protocols like SAML SSO, OAuth, OpenID Connect, Passive STS, and OpenID.</li> <li><b>Authentication Framework:</b> The central core, containing 'IN' (SP to local claim mapping, Local to IdP claim mapping) and 'OUT' (Local to SP claim mapping, IdP to Local claim mapping) processes, along with JIT Provisioning and XACML.</li> <li><b>Local Authenticators:</b> Includes Username/Password and TWA.</li> <li><b>Federated Authenticators:</b> Lists OpenID, OpenID Connect, OAuth, SAML SSO, Passive STS, Facebook, Yahoo, Google, and Microsoft.</li> <li><b>External Applications:</b> Shows logos for Facebook, Yahoo!, and Google.</li> <li><b>Outbound Provisioning:</b> Lists SCIM, SPML, Google, and Salesforce.</li> <li><b>Provisioning Framework:</b> Includes Identity Manager and Auditing.</li> <li><b>Inbound Provisioning:</b> Lists SOAP and SCIM.</li> <li><b>Authorization Manager, User Store Manager, and Claim Manager:</b> These are supported by LDAP, AD, and JDBC databases.</li> </ul> </p>
<b>Category</b>	Mandatory	<i>Technical.</i>
<b>SALT Topics</b>	Mandatory	Authentication and identity management
<b>Stage</b>	Optional	<ul style="list-style-type: none"> <li>• <b>design:</b> elaboration of the system design according to the different requirements;</li> <li>• <b>development:</b> implementation of the system based on the defined specification;</li> <li>• <b>deployment:</b> set up the system in the stakeholder's environment;</li> <li>• <b>operation &amp; maintenance:</b> use the system and ensure its correct functioning to satisfy stakeholder's needs;</li> </ul>
<b>Keywords</b>	Optional	Authentication, identity management, interoperability
<b>Guidelines</b>	Optional	There must exist at least one element within the system design model associated to the stereotype «AIM».
<b>OCL Rules</b>	Optional	<p>Interoperability.1              context Class inv Interoperability.1              ParisProfile::Legal::AIM::allInstances()-&gt;size()&gt;=1</p>

### 8.4 Reuse possibilities of the WP6 references

An equivalent document to this one has been produced in the frame of the WP6: it contains an indicative list of references dedicated to the biometrics use-case. The biometrics system that has been especially focused on in PARIS is a soft-biometry system using cameras as sensor. For this reason, many guidelines of any specie (Socio-Ethical, Technical, Legal) may be applied to both of the systems types.

This is of great interest because this also enables to show how the selection of applicable SALT data is realized for each of the use cases (among a consequent amount of available data): especially, SALT references are to be selected for each use case. A key selection parameter here

will simply be the country where the use case is considered to be placed, as it is France for WP5 and Spain for WP6.

All of the references that are listed in the WP6 document can be considered as valid for video-surveillance systems (for extensive contents of the references, please refer to the WP6 document), except those explicitly dedicated to biometrics systems, which are:

- The Opinion 3/2012 on the development of biometrics systems,
- Privacy by design solution for biometrics one-to-many identification systems

## 9 Appendix C: Mapping of ISO principles and SALT legal topics

ISO principles refers to the principles listed in ISO Standard 29100.

SALT Legal topics are based on the 95/46/EC Directive and are intended to ease legal analysis and legal compliance checks.

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