This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 720417

SURVANT

Surveillance video archives investigation assistant

D1.3 - Privacy, ethical and legal constraints

WP number and title	WP1 – Project Management
Lead Beneficiary	CERTH
Contributor(s)	ENG, ADM
Deliverable type	Report
Planned delivery date	30/06/2017
Last Update	24/07/2017
Dissemination level	PU

SURVANT Project

H2020-FTI-Pilot-2015-1 – *Fast Track to Innovation*
Grant Agreement n°: 720417
Start date of project: 1 January 2017
Duration: 24 months

Disclaimer

The SURVANT Consortium consists of the following partners:

	Partner Name	Short name	Country
1	Engineering Ingegneria Informatica S.p.A.	ENG	Italy
2	Ethniko Kentro Erevnas Kai Technologikis Anaptyxis	CERTH	Greece
3	Innovation Engineering srl	INNEN	Italy
4	United Technology Research Centre Ireland, Limited	UTRC	Ireland
5	Ayuntamiento de Madrid	ADM	Spain

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V0.1	19/04/2017	Draft	CERTH	ToC
V0.2	28/04/2017	Draft	CERTH, ENG, ADM	Final ToC
V0.3	06/06/2017	Draft	CERTH	First draft
V0.4	20/06/2017	Draft	CERTH, ENG, ADM	First complete draft
V0.5	26/06/2017	Completed version	CERTH	Version ready for peer review
V0.6	14/07/2017	Completed version	CERTH	Revised version
V0.7	19/07/2017	Completed version	CERTH	Additions in Section 2
V1.0	20/07/2017	Completed version	CERTH	Ready for peer review
V1.1	24/07/2017	Completed version	ENG	Final document for submission

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
CoE	Council of Europe
CFR	The Charter of Fundamental Rights of the EU
CNN	Convolutional Neural Networks
DL	Deep Learning
DPA	Data Protection Authority
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation
LEA	Law Enforcement Agency
LEP	Privacy, Ethical and Legal
OECD	Organisation for Economic Co-operation and Development
OWL	Web Ontology Language
PbD	Privacy by design
PETs	Privacy Enhancing Technologies
PII	Personally Identifiable Information
RNN	Recurrent Neural Networks
SURVANT	SURveillance Video Archives iNvestigation assisTant
SWRL	Semantic Web Rule Language
TEU	Treaty on European Union
TFEU	Treaty on the functioning of the European Union

Table of Contents

List of Figures

List of Tables

Executive Summary

Analysis and monitoring of Privacy, Ethical and Legal (LEP) constraints in SURVANT will be conducted within Task 1.3. The task's primary objective consists of two complementary parts: first, ensuring that R&D activities within the project will be compliant to respective laws and ethical practices, second, supporting system development so that the SURVANT system does not generate ethically unwanted effects, is respectful of human rights, and complies with the applicable legislation. It must be noted that, since SURVANT is the follow up of the research project ADVISE, the intention of the analyses within T1.3 is to build upon the ethical/legal work done within ADVISE.

The scope of the analyses within T1.3 is the SURVANT project and system and its context. For example, regarding data collection, since the SURVANT system is envisioned not as a video (data) collection tool but as a video analysis toolset, all ethical/legal obligations related to the data capturing phase of the data lifetime lie primarily with the initial owner/creator of the data.

The initial stage of the analysis was the preparation of an overview of ethical issues related to video surveillance as well as the applicable legal frameworks (international and European). At the heart of the ethical analysis lie the concepts of privacy and data protection which are analysed. Similarly, international and European legal frameworks for the protection of privacy and personal data are presented and analysed. A significant aspect of the SURVANT project is that it will be running in parallel with the fundamental change of the EU regulatory and legal framework which is taking place currently. The new Regulation (EU) 2016/679 shall apply from 25 May 2018 while the new Directive (EU) 2016/680 has to be transposed into national law of the EU Member States by 6 May 2018 (M17 out of 24 of the project). As a consequence, the SURVANT project will partly run with the previous EU privacy/ data protection framework in force (up to M17) and partly with the new EU privacy/ data protection framework in force (after M17).

A significant part of the present document and of the effort within T1.3 is devoted in identifying and describing the key differences between SURVANT and ADVISE that are considered to affect LEP aspects. The differences are presented in this document separated in *differences in what the system will be required to do* and *differences in how the system will do what is required*.

Finally, besides providing an overview of LEP principles that are relevant in the context of SURVANT and supporting the development of an ethically and legally compliant system, T1.3 team is also tasked with monitoring R&D activities with regards to LEP compliance. Therefore, we want to make sure that data processing conducted within SURVANT will be respectful of any personal data that might be included in the project datasets. To this end, a detailed discussion regarding the project datasets is presented in this document.

1 Introduction

Analysis and monitoring of Privacy, Ethical and Legal (LEP) constraints in the 'SURveillance Video Archives iNvestigation assisTant' (SURVANT) project will be conducted within Task 1.3 'Analysis and monitoring of privacy, ethical and legal constraints' of WP1 'Project Management'.

The task's primary objective consists of two complementary parts. First, ensuring that research and development activities within the project (mainly management[1] of datasets) will be compliant to respective National and European laws, and best ethical practices and rules/standards. Second, support the project consortium in developing a technical prototype, i.e. the SURVANT system, that does not generate ethically unwanted personal or social effects, is respectful of human rights (particularly the right to privacy and data protection), and complies to the applicable National and European legislation.

The analyses will, on the one hand, monitor research and development activities within the project with regards to respective laws, and best ethical practices, and on the other hand, identify any legal requirements applicable to the technical system and architecture itself and monitor their implementation.

It must be noted that, since SURVANT is the follow up of the research project ADVISE (GA 285024)[2] aiming to prove the ADVISE system at operational environment and commercialize it, the intention of the analyses within T1.3 is to build upon the respective work done within the ADVISE project and identify only additional or redundant requirements in comparison to the ones identified within ADVISE, for the SURVANT technical system and architecture.

In *Section 2* of this deliverable we provide an overview of privacy, legal and ethical rules and principles that are relevant in the context of the SURVANT project. We define the scope of our analysis, present international as well as European frameworks and best practices. *Section 3* provides a high-level capture of the key differences between SURVANT and ADVISE that are considered to affect LEP aspects. *Section 4* deals with ethical, legal and privacy monitoring of research and development activities focusing on the management of the datasets that are planned to be used in the project. Finally, the document concludes with *Section 5*.

Section 6 provides a list of all references to the text while *Annexes I and II* present consent form templates for the ADVISE and SURVANT projects.

[1] The term 'management' is used here in a sense that covers the whole dataset lifetime, from inception to creation/discovery and to long term storage or proper destruction.

[2] Advanced Video Surveillance archives search Engine for security applications (ADVISE, GA 285024), co-financed by EU in the FP7 Work programme in the SEC-2011 call. For more details please refer to: http://cordis.europa.eu/project/rcn/102502_en.html.

2 Overview of relevant LEP principles

This section provides an overview of privacy, legal and ethical rules and principles that are relevant in the context of the SURVANT project.

2.1 Scope of the analysis

SURVANT – SURveillance Video Archives iNvestigation assisTant – is a research project co-funded by the Horizon 2020 Framework Programme of the European Union.

All around the world, organizations and agencies deploy video surveillance to monitor and protect property and public infrastructure, driven by numerous factors like increasing crime rate, security threats, terrorism acts and even monitoring of law enforcement. The influx of surveillance footage from a growing number of cameras operating at higher resolutions, such as HD, coupled with the desire to increase the retention time of that footage is exploding the volume of the footage available. Organizations that have invested heavily in surveillance infrastructure are keen to exploit it for the automation of surveillance procedures using video analytics solutions.

SURVANT aims to deliver an innovative system that will collect relevant (i.e. surveillance) videos from heterogeneous repositories, extract video analytics, enrich the analytics using reasoning and inference technologies, and offer a unified search interface to the user. The SURVANT system functionality will be primarily adjusted for Law Enforcement Agencies (LEAs), critical infrastructure operators and private security organizations but the project will also try to adjust the system to other users that share common needs.

SURVANT is the follow up of the research project ADVISE (GA 285024), co-financed by EU in the FP7 Work programme in the SEC-2011 call. It intends to commercialise the results achieved in ADVISE and prove the final system at operational environment (TRL9).

2.1.1 Data Collection

Current procedures for performing investigations in video archives are cumbersome and time consuming. The investigator has either to collect all the relevant video footage in one place or identify the videos one by one and access them in a dedicated interface. In multi-camera environments, the investigator is usually forced to identify the exact camera location and viewing angle utilizing separate resources, limiting the overall situational awareness.

Existing video surveillance managing systems focus on real time operations, disregarding the challenges of video archive search. Their provision to assist investigators during search is limited to thumbnail extraction to speed up the detection of relevant segments, visualization of the location of the viewed camera and creation of custom playlists to assist investigation.

SURVANT aims to provide a unified interface for advanced, content-based search capabilities, evidence mining and smart investigation assistance functionalities, within collections of multiple video archives. The SURVANT system is envisioned not as a video (data) collection tool but as a video analysis toolset, especially efficient for very large volumes of video data coming from heterogenous sources (i.e. cameras or surveillance systems of different specifications and technologies).

Therefore, all ethical/legal obligations related to the data capturing phase of the data lifetime lie primarily with the initial owner/creator of the data (e.g. legal surveillance, notification of by passers etc.). Of course, the SURVANT system will be subsequently processing[3] these enormous amounts of videos and must therefore comply to all legal and ethical rules that have to do with the processing of such data (that might be also including personal[4] or even sensitive[5] data).

2.1.2 Data Analysis

2.1.2.1 Automated Analyses

The SURVANT system will perform video (and image) analysis employing Deep Learning (DL) techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), used to analyse static and motion content respectively. Inter-camera tracking and re-identification (of detected content) will be at the core of attention. Optimal balance between speed and accuracy will be pursued. *DL systems have been already successfully deployed in applications such as object classification, object detection and tracking, activity recognition and modelling etc. They are already deployed in commercial applications enabling new functionalities due to impressive performance.* Especially regarding indexing of the content (video and images), SURVANT will use advanced multimedia indexing tools (e.g. such as those developed by the EU-FP7 LASIE project[6]) that will be leveraged and validated for larger scale deployments.

The SURVANT system will also apply event enrichment and reasoning. It will deliver an inference framework able to combine together low-level information and semantic annotations to enable automated reasoning mechanisms to discover high-level events and/or investigative hypotheses. Specifically, SURVANT will evolve the OWL tableau reasoning framework developed in ADVISE, based on a SWRL (Semantic Web Rule Language) approach, applying the event calculus formalism in order to allow the event reconstruction in a narrative way taking into account spatial-temporal coordinates useful to track the crime and predict its evolution in the time and space. OWL reasoning parallelization using concurrent computation of inherently independent proof steps will be utilized to optimize performance and ensure the scalability of the system.

---

[3] According to the [General Data Protection Regulation]: *"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

[4] According to the [General Data Protection Regulation]: *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

[5] In general, EU legislation identifies special categories of personal data that are subject to additional protections, i.e. 'sensitive (personal) data'. According to [Directive 95/46/EC]: *"'sensitive (personal) data' are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life."* According to the [General Data Protection Regulation]: *"'sensitive (personal) data' are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence)."*

[6] Large Scale Information Exploitation of Forensic Data (LASIE), EU FP7 IP, http://www.lasie-project.eu/.

2.1.2.2 Nonautomated Analyses

Finally, in contrast to the above automated analyses, the SURVANT system will also leverage human intervention (human-in-the-loop) capabilities – such as GIS-based GUI allowing the user to execute targeted queries, advanced relevant feedback tools, etc – and augment them with a more user-friendly multimodal interface and more advanced reasoning capabilities. Topology-driven reasoning will have a key role in learning from the trajectory of temporal events (the geographic positions of the retrieved events) and provide recommendations to the user.

2.1.3 Validation

The SURVANT system will be validated through live prototype demonstrations (pilot tests) in LEA operational environment.

2.2 Overview of the ethical issues related to video surveillance

A concise but yet complete list of key ethical issues related to video surveillance has been provided in Deliverable 2.2 'Report of relevant legal and normative standards and their evolution' of the ADVISE project [ADVISE D2.2]:

- **Privacy and the person.** The primary ethical issue invoked by surveillance activities in general is that of privacy. Privacy in ethical terms invokes the notion that there is a sacrosanct "person" at the core of any and every object of human surveillance. This person is different than the information about the person gathered through surveillance and cannot be reduced to the surveillance data.
- **Sub-categories of privacy** (e.g. privacy of the body, of personal behaviour, of communication, of personal data etc) are the subject of ethical debate and no definitive categorisation exists.
- **Criteria for assessing invasiveness** (in terms of privacy violation) of a specific surveilance action or technology can vary according to context.
- **Data protection** – from an ethics point of view – concerns the means available to safeguard privacy and invokes several issues such as: *the actual data* that is collected and stored, *storage conditions*, *duration of storage*, *metadata*, *informed consent* (or, in other words, authorisation by the subject whose data is being processed for the processing of the data), *risk assessment* (of the possibilities and consequences of data theft, disclosure etc), *(DPA) notification requirements* as per national or European law, *dual use* (i.e. unintended secondary use) of the data, and *proportionality* as the governing principle indicating that only data necessary to the end envisaged should be collected and not more.
- **Biometric data** generate several problems that are not yet adequately covered by EU regulations.
- **Fundamental rights** of the person[7].

It is worth noting that guarantees of privacy are central tenets of the European Charter for Fundamental Rights [CFR] and emerge from a deontological[8] approach to ethics that places the interests and rights of the individual at the forefront. The European Commission has taken steps to safeguard and attempt to guarantee personal privacy. This is evidenced by the new General Data Protection Regulation (GDPR)

[7] E.g. the Charter of Fundamental Rights of the European Union enshrines certain political, social, and economic rights for European Union (EU) citizens and residents into EU law.

[8] Deontology (also referred to as Kantian ethics) is based on moral beliefs and values and, the obligations of the individual towards others. Often used in contrast to Teleology, i.e. results-oriented ethics that determines an action to be ethically sound if its results produce benefits and happiness for others.

[GDPR] that sets out new rules deemed to be 'future-proof', the aims of which are to protect the personal data of individuals.

2.2.1 The concepts of privacy and data protection

In the classical understanding, ***privacy*** is usually defined as the ability of an individual to be left alone, out of public view, free from surveillance or interference from others (individuals, organisations or the state) and in control of information about oneself. However, while privacy sets prohibitive limits that shield the individual against the state, public authorities and other powers, ***data protection*** controls legitimate use of such power, imposing a certain level of transparency and accountability. In other words, data protection controls and channels legitimate processing of personal data.

Hence, privacy and data protection are not equivalents. There is a substantive difference between these two. On the one hand, privacy is broader than data protection; the latter is just a tool to protect the former. On the other hand, while both fundamental rights – to privacy and to data protection – participate in the protection of the political private sphere, this is done in separate ways; privacy sets prohibitive limits that shield the individual against public authorities and other powers (warranting a certain level of opacity of the citizen), whilst data protection channels legitimate use of power (imposing a certain level of transparency and accountability). [PRESCIENT D1]

2.3 Legal frameworks for the protection of privacy and of personal data

2.3.1 Protection of privacy

At the international level, the right to privacy is protected by Art 12 of the Universal Declaration of Human Rights (1948) [UDHR], however non-binding. Art 17 of the International Covenant on Civil and Political Rights (1966) [ICCPR], i.e. a binding international human rights instrument, offers protection of privacy. In 1980, the Organisation for Economic Cooperation and Development (OECD) issued (and revised in 2013) the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (non-binding) [OECD Privacy].

Protection of privacy at the European (regional) level is based on two systems:

- The first one, i.e. *the Council of Europe (CoE)*, is based on Art 8 of the European Convention on Human Rights (ECHR) [ECHR]. The ECHR establishes the European Court of Human Rights (ECtHR) in Strasbourg. While the ECHR itself is silent about protection of personal data, the Court has developed it from the right to privacy.
- The second one, i.e. *the European Union*, is based on Art 7 CFR. However, the scope of the CFR is limited to "the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law" (Art 52(1) CFR).

2.3.2 Protection of personal data

When it comes to personal data, protection in the European (regional) level is again based on two systems:

- For the first system, i.e. *the Council of Europe (CoE)*, there is the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No 108) with an additional protocol regarding supervisory authorities and transborder data flows (No 181).

- The other system, i.e. *the European Union*, is based on its Treaties (TEU and TFEU), the Charter of the Fundamental Rights (CFR) and secondary legislation, namely the Directives.

Basic instruments of EU legislation on the mater are:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*known simply as the 1995 Data Protection Directive or Directive 95/46/EC*).
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
- Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (i.e. lying down data protection rules applicable only for the EU institutions and bodies).

2.3.2.1 EU data protection framework

The core instrument for data protection in the European Union is the well-known 1995 Data Protection Directive. Directive 95/46/EC sets up a three-level system for the protection of personal data. The first level is the general one that applies to any processing of personal data. The second level, which needs to be applied on top of the first level, is applicable when sensitive data are being processed. The third level is applicable when personal data are being processed to third countries, i.e. outside the European Union/European Economic Area.

This Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of (former) Community law and by a natural person in the course of a purely personal or household activity.

As a directive is an EU legal instrument that is not directly applicable in the Member States, each of them needed to implement it in their legal systems. ***Therefore, we have at least 27 national laws governing data protection in the EU.***

Directive 95/46/EC uses four core definitions:

__Personal data__ shall mean "any information relating to an identified or identifiable natural person" (i.e. the data subject).

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 physical, physiological, mental, economic, cultural or social identity."

---

*The **data controller** is a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."*

*The **data processor** is "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."*

2.3.3 EU data protection reform

The SURVANT project is planned to be running for two years, that is between January 2017 and December 2018. ***A fundamental change of the EU regulatory and legal framework is taking place within that period.***

In January 2012, the European Commission put forward an EU Data Protection Reform aiming "to make Europe fit for the digital age".

On 15 December 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules, establishing a modern and harmonised data protection framework across the EU. The European Parliament's Civil Liberties committee and the Permanent Representatives Committee (Coreper) of the Council then approved the agreements with very large majorities. The agreements were also welcomed by the European Council of 17-18 December as a major step forward in the implementation of the Digital Single Market Strategy.

On 8 April 2016, the Council adopted the Regulation and the Directive. And on 14 April 2016 the Regulation and the Directive were adopted by the European Parliament.

On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages:

- **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). – http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
- **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. – http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG

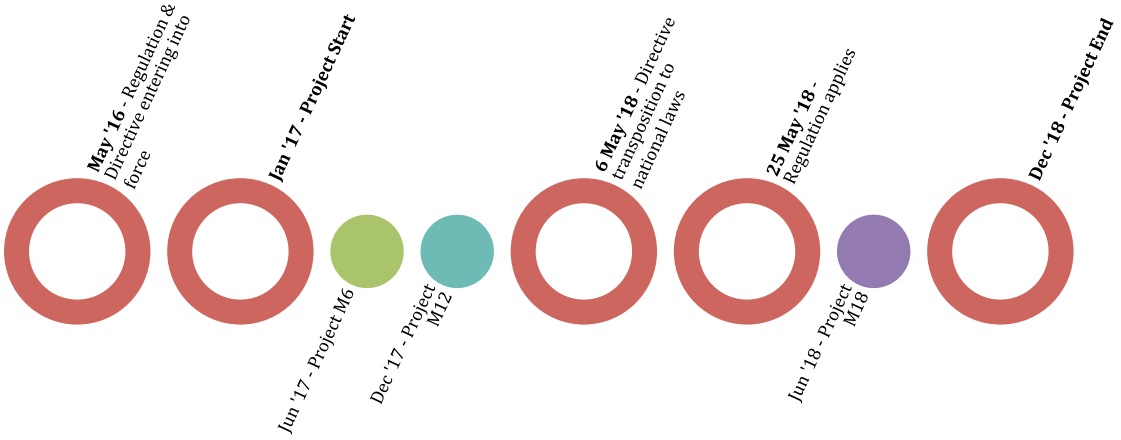

Figure 1: EU data protection reform timeline.

While the Regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018.

The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy.

2.3.3.1 An overview of the main changes under GPDR and how they differ from the previous directive

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The enforcement date of the GDPR is 25 May 2018 at which time those organizations in non-compliance will face heavy fines.

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies. Key changes related to the SURVANT project can be found below:

- **Increased Territorial Scope (extra-territorial applicability).** Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.
- **Penalties.** Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
- **Consent.** The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given

in an intelligible and easily accessible form, with the purpose for data processing attached to that consent.

- **Right to Access.** Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.
- **Right to be Forgotten.** Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.
- **Privacy by Design.** Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. *The ADVISE and SURVANT projects had Privacy by Design in their core from the very beginning.*
- **Data Protection Officers.** Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:
    - Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
    - May be a staff member or an external service provider
    - Contact details must be provided to the relevant DPA
    - Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
    - Must report directly to the highest level of management
    - Must not carry out any other tasks that could results in a conflict of interest.

2.4 Best practices for protecting privacy and personal data

Several tools and methodologies exist that can be used either for ensuring privacy/ personal data protection or for monitoring the impact of a system with regards to legal, ethical and privacy principles.

2.4.1 Privacy by design

Privacy by design (PbD) is a concept developed and subsequently promoted by Dr Ann Cavoukian, the Information and Privacy Commissioner of Ontario, in 1990s, to address the ever-growing and systemic effects of information and communication technologies (ICT), and of large-scale networked data systems. Davies observed that the emergence of privacy by design presents a substantial opportunity to raise the bar on privacy protection and to reduce the extent of surveillance of people's data and transactions. Privacy by design advances the view that the future of privacy cannot be assured solely by compliance with regulatory

frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. [Davies]

2.4.2 Privacy Enhancing Technologies

Privacy Enhancing Technologies (PETs) are technologies that are designed for supporting privacy and data protection. The objective of PETs is to protect personal data and ensure the users of technology that their information is confidential and that management of data protection is a priority to the organizations who withhold responsibility for any personally identifiable information (PII). PETs address among other the principles of data minimisation, anonymisation and pseudonymisation. Examples of PETs are communication anonymizers, encryption tools, cookie-cutters, etc.

2.4.3 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a process which assists organizations in identifying and minimizing the privacy risks of new products, projects or policies. The organization audits its own processes and sees how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes. A PIA is designed to accomplish mainly three goals:

- Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
- Determine the risks and effects; and
- Evaluate protections and alternative processes to mitigate potential privacy risks.

PIAs are considered a good means to address challenges posed by emerging technologies and in particular, video surveillance. [Raab et al]

A number of PIA methodologies and templates have been developed to help organisations carrying out a PIA.

3 Key differences between SURVANT and ADVISE affecting LEP aspects

This chapter provides a high-level capture of the key differences between SURVANT and ADVISE that are considered to affect LEP aspects. The differences are separated into differences in requirements (user, system etc.), or in other words *differences in what the system will be required to do*, and purely technical differences (e.g. architectural differences or differences in specific modules), or in other words *differences in how the system will do what is required*.

3.1 Differences in requirements

3.1.1 Use Cases

Commercially focused use cases have been de-prioritized in SURVANT. ADVISE tackled three use cases of criminal activity on commercial premises – vandalism of company property (graffiti, fuel theft and car vandalism in car parks). In SURVANT we recognise that criminal incidents on commercial premises are just particular scenarios of use cases observed in the community. The same use cases are valid for street surveillance but here the circumstances are generally more challenging with a larger diversity of cameras and busier scenes. Tackling the more challenging scenarios that occur in uncontrolled environments promises to deliver a more robust platform that offers increased reusability across street and commercial surveillance.

The focus of SURVANT has shifted to use cases and scenarios that offer good reuse across sectors and for which the consortium can leverage decent quality training footage staged with actors in real life challenging environments.

3.1.2 Investigation areas of focus

We have learned that investigators routinely request surveillance footage that encompasses bigger spatial and temporal areas than the actual time and place of the reported incident. Investigators are not only interested in the actual scene of the crime but also in activities in the surrounding area in the times immediately preceding and following the incident. The reasons for this include:

- Poor surveillance footage of the area where the incident actually occurred where definitive suspect identification is difficult
- Identification of accomplices that may become evident as they accompany the suspect in nearby areas before and/or after the crime
- Construction of an incident timeline which captures the geographical and temporal path of the victim and/or suspect(s)

ADVISE works under the principle that an investigator identifies a time and area and then it analyses this entire area and time period for evidence of a particular event. Not only does this result in needless analysis of footage for event detection (e.g. looking for evidence of pick pocketing in block B when we know it occurred in block A) but it also increases the amount of information clutter presented to the end user.

In SURVANT we recognise the investigator's dual intent of firstly analysing a specific incident area where the crime occurred and secondly, analysing a surrounding time and area for the presence of particular

objects (people, cars). To this end we allow investigators to identify an explicit incident zone and a wider analysis zone. The incident zone is used to capture the suspect on film which is then used to seed a search of the suspect in the wider analysis zone.

3.1.3 Repository Management

ADVISE worked under the principle that each cameras is attached to a single repository. Multiple cameras may be attached to the same repository. When investigators include a camera in an investigation they specify a time period and ADVISE would then query the associated camera repository for that subset of footage. In discussions with the end user we discovered that repositories are actually assembled per investigation. The base repository to which street surveillance cameras are connected to is strictly controlled by an official video controller within the LEA organisation. Access to subsets of footage within this repository are only given to investigators upon presentation of official authorization by a high ranking LEA. In effect, investigators are given smaller bespoke repositories which are extracted from the main repository. A similar principle applies to commercial surveillance footage – subsets of footage are extracted by commercial organisations and handed over to investigators upon official request. We observed, therefore, that the data available to SURVANT is dispersed across a large and dynamic collection of small independent repositories rather than concentrated in a small number of large integrated repositories.

We can see the same pattern with mobile phones and other portable video devices where captured footage does not all exist in a single repository but is instead downloaded and managed in small individual repositories.

A new model of repository management is proposed for SURVANT in which bespoke repositories are identified and attached to an investigation. This model has the benefit of preventing data leakage between investigations as access is limited to the data explicitly attached to a given investigation

3.1.4 Facility to search for people without criminal incident

ADVISE was based on the premise that there was an explicit criminal incident but there are cases where surveillance footage needs to be analysed based on a particular physical location (to observe who visits a certain building for example) or the last sighting of a particular person (elderly person with Alzheimer's for example).

3.1.5 Anonymization as optional

In ADVISE, anonymization of surveillance footage was an integral part of the processing pipeline. Discussions with investigators revealed that this is unnecessary (and often unwelcome). SURVANT will make the anonymization step optional – a configuration setting that can be enabled or disabled by the SURVANT platform administrator.

3.2 Technical differences

3.2.1 Differences in Architecture

SURVANT's main purpose is to develop a system that will be ready for the market using as a starting point the system developed in the EU FP7 project ADVISE. Its architecture is based on the ADVISE architecture but it integrates some essential changes that will render the system ready for use in a real-world

environment. The architectural differences, as well as the evolved parts, aiming to improve performance, efficiency and a user intuitive interface are presented in this section.

The main difference between the two projects is about the software design. While ADVISE follows a monolithic design, SURVANT is being developed as a micro-service multi-container application. A monolith is a software shipped as a single big block and its parts show a high degree of coupling, which means that they have many dependencies among themselves with the disadvantage that if the developers want to apply any modification to the platform they have to build and redeploy the whole software. On the contrary, micro-services are low in coupling and high in cohesion: they are self-contained components with zero or very low dependencies among them, devised to meet per-business requirements. The main advantages of this architecture are summarized here:

- Self-contained modules are prone to reusability.
- The whole system is more robust because the lack of dependencies between modules implies that the failure of one of them doesn't affect the integrity of the others.
- Micro-services can be scaled easily (they are actually made for being scaled out), scaling a monolithic application can be a painful challenge.
- Once the interface among micro-services has been decided, micro-services can be implemented using different technologies instead of adopting a unique framework for the whole application like happens in monolithic applications.

Here is an in-depth sight into SURVANT and ADVISE architectures.

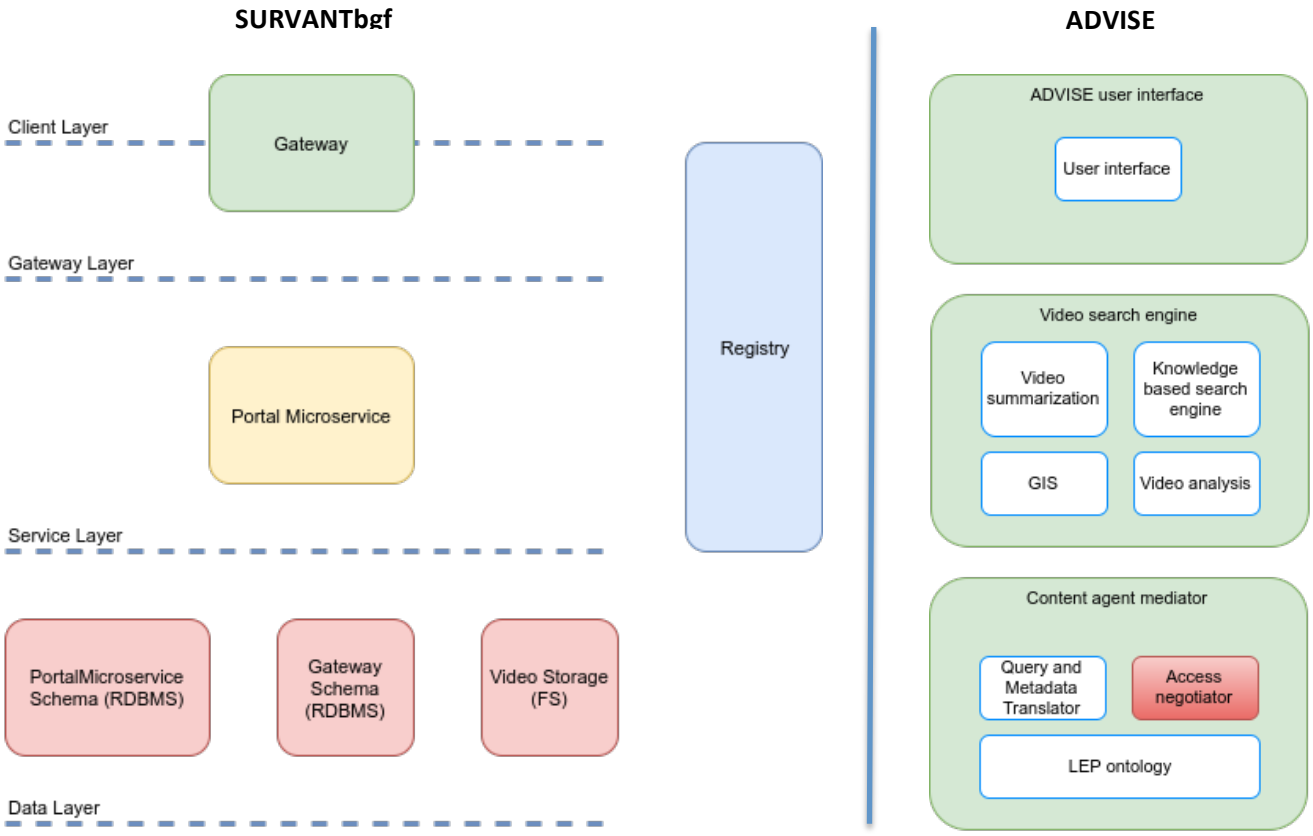

Figure 2: Comparison of the logical architecture of SURVANT (left) and ADVISE (right).

Analysing the diagrams from the top, the first difference can be found in the implementation of the user interface logical blocks. While ADVISE has a "legacy" user interface design, SURVANT inherits the characteristics of the Backend-For-Frontend (BFF) architectural paradigm that helps to tailor a backend system for end-user interfaces, enhancing the user experience (the Gateway) on multiple devices such as mobile and web clients. This choice has been made to allow frontend developers to focus on their tasks without having to take into account other self-contained parts of the system. Moreover, the technological solutions employed don't affect other corresponding BFFs (if present).

Moving to the service layer, each working service such as the GIS and the Video Analysis is going to be decoupled, improved and containerized according to the micro-service specification, earning all the advantages described above. SURVANT will use Docker containers to host each micro-service to take advantage of their flexibility, expandability and the easy management they offer. This choice allows to easily deploy the SURVANT system in client infrastructure without having to worry about system specific problems and dependencies. Moreover, it allows the deployment of multiple instances of the same services to improve system performance in the same or even remote infrastructure, assuring system expandability.

Another significant evolution consists in the fragmentation of the responsibilities of the Content access negotiator across all the micro-services. This means that the system doesn't have a centralized requests negotiator anymore, but each module implements independently the access to its own entities, in accordance to the kind of user, the role, the permissions and the access level. Last but not least, the overall security in SURVANT is finely tuned because it implements the following additional components:

- User Authentication Authority Server: manages the authorization and the authentication of the users on the portal.
- Micro-services Access Control List: manages the authorization of the gateway in relationship with each registered micro-service.

3.2.2 Differences in Modules

The SURVANT system reuses the modules that have been identified and developed in ADVISE. However, most of them are re-designed to cover the requirements of the end-users. New technologies are employed to improve their efficiency and performance, extending in some cases their functionality. The following table illustrates the differences of each module in the two projects.

Modules	Functional modules	Type of change	Details
Video Processing	**Object detection & tracking**	Redesign	**Performance:** Employ Deep Learning techniques to improve object detection and tracking. **Speed**: Improve processing time to less than real time
	Event detection	Redesign	**Performance:** Employ Deep Learning techniques to improve event detection. Detect more events **Speed**: Improve processing time to less than real time
Indexing	**Visual Description**	Redesign	**Performance:** Employ Deep Learning techniques to extract more distinctive descriptors for objects detected.

	Indexing	Redesign	**Performance:** Improve query results **Speed:** Improve search time in the database
Anonymization	**Selective Anonymization**	Improve	**Performance:** Improve the anonymization process to hide unnecessary personal data during the investigation **Speed:** Provide on the fly anonymized video results.
Knowledge modelling	**Ontology**	Redesign	**Performance:** Improve the expressiveness and flexibility of the ADVISE ontology to better model the knowledge extracted from the videos examined.
Geographical analysis	**Spatial Reasoner**	Redesign	**Performance:** Improve reasoning capabilities using spatio-temporal constraints combined with similarity metrics (what, where, when workflow)
	Trajectory Mining	New	**Performance:** Improve Re-Identification using geographical trajectories
Reasoning	**Rule based reasoning engine**	Improve	**Performance:** Improve the expressivity capabilities of the system for more complex rules **Speed:** Faster reasoning capabilities
	Probabilistic Rule Engine	New	**Performance:** Allow the creation of elastic rules for complex events that are based on probabilities
	Rules from examples	New	**Performance:** Allow the creation of rules based on examples
Complex query	**Query Formulator**	Redesign	**Performance:** Allow the creation of queries from multiple modalities and the use of filtering operators
	Cross modal query expansion	New	**Performance:** Allow the expansion of queries in modalities different from the original one
Services & Applications	**Portal micro-service**	Improve	**Performance:** Investigations and related entities are self-contained
	Search by Image	New	**Performance:** Enables the user to address the search process straight to a specific feature
	Event summarizer	Improve	**Speed:** Offers an overview of the relevant detected events extracted by a video at a glance.
Visualization	**Natural Query UI**	Improve	**Performance:** Allows the user to compose queries more intuitively
	Gateway	Improve	**Speed:** The “one-page application” structure improves the responsiveness of the user interface improving the overall user experience.

Table 1: Module differences between ADVISE and SURVANT.

4 Monitoring of privacy, ethical and legal constraints

Besides providing an overview of LEP principles that are relevant in the context of the SURVANT project and supporting the project consortium in developing an ethically and legally compliant technical prototype, i.e. the SURVANT system, Task 1.3 also aims in monitoring research and development activities throughout the project with regards to respective laws and best ethical practices and making sure that privacy, ethical and legal principles are respected.

To this end, we want to make sure that data processing that will be conducted by the SURVANT consortium during the project is respectful of any personal data that might be included in the project datasets. The SURVANT project is planning to use two datasets:

- The ADVISE dataset, inherited by the ADVISE project, and
- The SURVANT dataset, which will be created within the SURVANT project

The two datasets as well as all the procedures followed in order to capture these datasets are described ni the following sections.

The key points that are important in terms of legal/ethical compliance are that:

- Both datasets were/ will be created within the controlled environment of a European research project (ADVISE in the first case, SURVANT in the second case) and within a control physical space (areas within or right next to the premises of Madrid Municipal Police or areas controlled by the Madrid Municipal Police)
- Both datasets were/ will be staged, meaning that only volunteer 'actors' are depicted in the videos comprising the datasets and no other person is depicted; this ensures that all people depicted in the videos comprising the datasets are aware of their participation and no one is depicted despite his will.
- All 'actors' participating in the videos comprising the datasets have signed/ will sign an appropriate consent form for their participation in research activities (i.e. participation in the video capturing). The Consent Form template that will be used in the SURVANT project can found in Annex II.
- Proper agreements have been signed between the initial owner of the ADVISE dataset (the partner that captured it) and the rest of the ADVISE project consortium regarding the use of the dataset. The sane procedure is envisioned for the case of the SURVANT dataset and it is the responsibility of Task 1.3 to monitor that this procedure is conducted appropriately and completed in a timely manner (i.e. before the actual processing of the dataset by technical partners of the consortium commences).

4.1 ADVISE Dataset

In the municipality of Madrid, CCTV cameras are controlled by municipal police and accessible locally at each of the locations where they are installed. All signals received from the locations where CCTV cameras are located, are centralized in the Integrated Centre for Video Signal (CISEVI). For the purpose of the ADVISE project, the Madrid Municipal Police performed video recordings using the available infrastructure of cameras deployed in the city. The only way to ensure that recordings would match the identified use cases was to record them on purpose, that is, with actors making a representation, once and again, of the use cases. The Theatre Group of the Madrid Municipal Police performed the identified use cases for the benefit of the project. A total of 27 actors acted out with different clothing, cars, motorcycles, and luggage.

During the recordings, other people and vehicles were prohibited from entering the area. The recordings were taken with different light condition, different people, number of people, etc. to be as more realistic as possible. The police officers working at CISEVI were responsible for the recordings. The scenarios and use cases were "Pickpocketing", "Luggage theft" and "Beat and Run Away". The videos in the available infrastructure are securely saved in a proprietary format in CISEVI. For this reason, extracted videos were converted to AVI so that the technical partners could work with them. Furthermore, the videos recorded were examined from the Madrid Municipal Police to exclude segments where residents may accidentally appear in a scene. In total, 103 videos were produced in AVI format that contained multiple instantiations of the identified use case scenarios, as well as "no event" videos for training purposes. Ethical and Legal Aspects – as these have been shaped by partner ADM – were taken into consideration since the very beginning. The person, in Madrid City Council, responsible for video surveillance cameras deployed in the streets was adequately informed of the recordings for the project that were to take place. Moreover:

- All actors performing on the street had previously signed an appropriate Consent Form that was based on the template shown in Annex I.
- No other people, but the actors were shown on the recordings.
- A Memorandum of Understanding was signed between partner ENG, in the name of the whole Consortium, and partner ADM, for the usage of recordings.

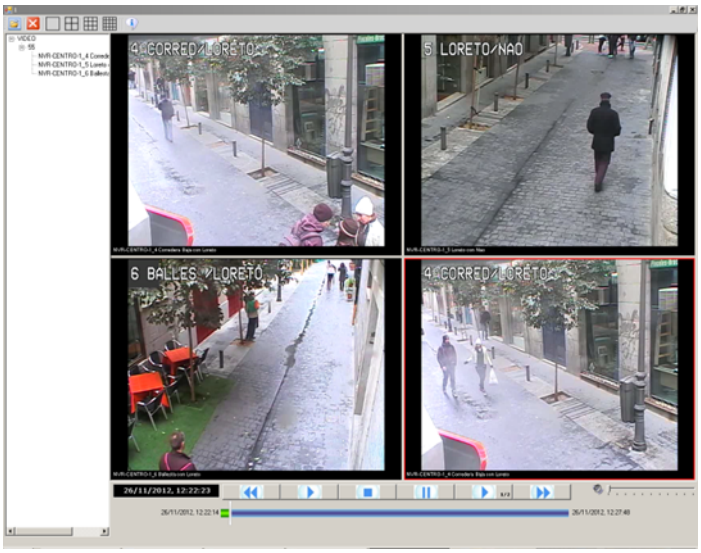

Figure 3: Videos contained in the ADVISE dataset.

4.2 SURVANT Dataset

The Madrid Municipal Police will perform new recordings for the SURVANT project that will be based on the use case scenarios identified in D2.1 "Requirements and use cases". The scenarios that have been identified are the following:

Storyline 1: Aggression on a street in Madrid. The aggressor ran away after beating several times in the face and the body of a tourist in an unprovoked attack, because the victim would not let go of the backpack the aggressor was trying to steal form him.
Storyline 2: Theft of a wallet with credit cards, documentation, and 625 euros from a city street in Madrid. The victim was a Japanese citizen who was traveling alone. A thief opened his backpack, removing his wallet from it, while another one (his companion) distracted him by offering cheap

sunglasses.
Storyline 3: Due to the confrontation between official city taxi drivers and new rental cars with driver (UBER, CABIFY), the later ones are suffering aggressions to their vehicles by taxi drivers, who throw stones and damage their cars. A taxi driver detects an unattended Uber car and gets off his own cab to make graffiti on the Uber. He spoils the car paint and leaves an offensive message at the same time. The taxi driver quickly drives away.
Storyline 4: A couple of youngsters armed with sprays in a not very busy street, and in just a few minutes, make graffiti on the wall of a public building, defacing its façade. They leave the area at a fast moving pace.
Storyline 5: The police know that in a particular building there is a possible jihadist group that meets in one of the apartments. The investigators want to monitor who enters and leaves the building during a period of time.
Storyline 6: The crime of assault on a tourist was captured on surveillance video but the footage is of insufficient quality to identify the attacker or all of their accomplices. Investigator examines surrounding footage to seek more information
Storyline 7: A vulnerable elderly person, affected with Alzheimer, has been reported missing. Last time he was seen near a shopping centre in a street near his house. He walks with the aid of a cane.

Based on the above scenarios, the Madrid Municipal Police will perform new recordings where officers will instantiate the above scenarios under various conditions. It will exploit its previous experience from the data acquisition and sharing process during the ADVISE project to deliver a dataset according to the relevant legal and ethical regulations. After negotiations with the relevant authorities, the Madrid Municipal Police has been authorized to perform the recordings in crowded areas to replicate the actual operational environment. In all cases, the events described in the scenarios will be instantiated by police officers only and not real cases.

Please note that the recordings have not taken place at the moment that this deliverable was being written. Therefore, no further details are available on the dataset to be acquired.

5 Conclusions

In this report, we presented the analyses and activities taking place within Task 1.3 “Analysis and monitoring of privacy, ethical and legal constraints” of the SURVANT project.

The analysis of LEP principles indicates that a major issue is the currently undergoing EU data protection reform which will oblige SURVANT to be partially run within two different data protection frameworks. Early adoption by the SURVANT consortium members of notions such as Privacy by Design and Privacy by Default even back from the beginning of the ADVISE project is a powerful tool that the project holds in order to cope with the coming changes. Another important aspect highlighted by the LEP analysis is that, since the SURVANT system is envisioned not as a video (data) collection tool but as a video analysis toolset, all ethical/legal obligations related to the data capturing phase of the data lifetime lie primarily with the initial owner/creator of the data

The analysis of key differences between SURVANT and ADVISE that affect LEP aspects indicated a shift from LEA focused use cases to scenarios that offer good reuse across sectors and for which the consortium can leverage decent quality training footage staged with actors in real life challenging environments. This change does not pose additional problems to the legal/ethical side since the envisioned system was initially designed with such cases in mind.

Finally, our LEP monitoring activities focused in identifying and describing the project datasets in order to be ready to ensure legal/ethical compliance regarding their management and of course the management of personal data that might be contained within. Both datasets are created within a controlled environment, are staged (meaning that only volunteer ‘actors’ participate), all ‘actors’ in both datasets are signing appropriate consent forms, and proper agreements are signed between initial owners of the datasets (the partner that captured it) and the rest of the partners.

6 References

[ADVISE D2.2] Deliverable 2.2 'Report of relevant legal and normative standards and their evolution', Advanced Video Surveillance archives search Engine for security applications (ADVISE) EC FP7 project (GA No. 284024), http://www.advise-project.eu/.

[CFR] Charter of Fundamental Rights of the European Union (the Charter in the latest (2012) consolidated version of the Lisbon Treaty), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:12012P/TXT.

[Davies] Simon Davies (2010) *Why Privacy by Design is the next crucial step for privacy protection*, Initiative for a Competitive Online Marketplace (ICOMP), p 13, http://www.i-comp.org/blog/wp-content/uploads/2010/10/privacy-by-design.pdf.

[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[ECHR] The Convention for the Protection of Human Rights and Fundamental Freedoms (better known as the European Convention on Human Rights), http://www.echr.coe.int/pages/home.aspx?p=basictexts.

[GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[General Data Protection Regulation] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

[ICCPR] International Covenant on Civil and Political Rights, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

[OECD Privacy] The Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as revised in 2013, http://www.oecd.org/sti/ieconomy/privacy.htm.

[PRESCIENT D1] Serge Gutwirth, Michael Friedewald, David Wright, Emilio Mordiniet al. (2010) *Legal, social, economic and ethical conceptualisations of privacy and data protection*, Deliverable D1 of the PRESCIENT project [Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment], p 8 and p 8ff, http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf.

[Raab et al] Charles Raab and David Wright (2012) *Surveillance: Extending the Limits of Privacy Impact Assessment*, in David Wright and Paul de Hert (eds.) Privacy Impact Assessment, pp 363-384

[UDHR] The Universal Declaration of Human Rights, http://www.un.org/en/universal-declaration-human-rights/.

7 Annex I – ADVISE Consent Form template

SAMPLE CONSENT FORM TO PARTICIPATE IN RESEARCH

Consent must be obtained from any study participant. Participants should be given two copies of the consent form – one to keep, and one to sign and return to the ADVISE Consortium.

CONSENT TO PARTICIPATE IN THE ADVISE PROJECT (SEC-2011.5.3-4, No.: 285024)

This is to state that I agree to participate in a program of research being conducted by the ADVISE Project: (Project Coordinator name: Francesco Saverio Nucci, Organization: ENGINEERING INGEGNERIA INFORMATICA SPA, Coordinator's Email: francesco.nucci@eng.it, Coordinator's Fax: +39 06-83074200).

A. PURPOSE

I have been informed that the purpose of the research is as follows: *{Please state the purpose of the research clearly and concisely, in no more than one or two sentences}*.

B. PROCEDURES

{Indicate in this section where the research will be conducted and describe in non-technical terms what the subjects will be required to do, the time required to do it, and any special safeguards being taken to protect the confidentiality or well being of the subject}

C. RISKS AND BENEFITS

{Indicate in this section all potential risks of participation and any benefits of participation}

D. CONDITIONS OF PARTICIPATION

- I understand that I am free to withdraw my consent and discontinue my participation at anytime without negative consequences.
- I understand that my participation in this study is *{pick appropriate word: CONFIDENTIAL (i.e., the researcher will know, but will not disclose my identity) OR NON-CONFIDENTIAL (i.e., my identity will be revealed in study results)}*.
- *{I understand that the data from this study may be published.*

OR

- *I understand that the data from this study will not be published.}*

I HAVE CAREFULLY STUDIED THE ABOVE AND UNDERSTAND THIS AGREEMENT. I FREELY CONSENT AND VOLUNTARILY AGREE TO PARTICIPATE IN THIS STUDY.

NAME _____

SIGNATURE _____

If at any time you have questions about the proposed research, please contact the project's Coordinator (Project Coordinator name: Francesco Saverio Nucci, Organization: ENGINEERING INGEGNERIA INFORMATICA SPA, Coordinator's Email: francesco.nucci@eng.it, Coordinator's Fax: +39 06-83074200).

If at any time you have questions about your rights as a research participant, please contact the project's Ethics Advisory Board *{Indicate in this section the name, and contact information for the Data Protection Controller}*.

8 Annex II – SURVANT Consent Form template

SURVANT (Ref.: 720417) Date: ___ / ___ / _____

CONSENT FORM TO PARTICIPATE IN RESEARCH

I hereby declare that I consent to participate in an experiment that will be conducted within the **SURVANT** research project as described below.

SURVANT, SURveillance Video Archives iNvestigation assisTant, H2020-FTIPilot-2015-1, IA, Ref.: 720417

– **Coordinator:** ENGINEERING - INGEGNERIA INFORMATICA SPA, Via San Martino Della Battaglia 56, 00185 ROMA, Italy (Giuseppe Vella, email: giuseppe.vella@eng.it).

A. PURPOSE

I have been informed that the purpose of the experiment is *{Please state the purpose of the research clearly and concisely, in no more than one or two sentences}*.

B. PROCEDURES

{Please indicate where the research will be conducted and describe in non-technical terms what the subject will be required to do, the time required to do it, and any special safeguards being taken to protect the confidentiality or wellbeing of the subject}.

C. RISKS AND BENEFITS

{Please indicate all potential risks and/or benefits of participation for the subject}.

D. CONDITIONS OF PARTICIPATION

- **I understand that** I am free to withdraw my consent and discontinue my participation at any time without negative consequences. At such case, all collected data corresponding to my participation will be deleted and a proof of deletion will be presented to me.
- **I understand that** my participation in this study is *{please pick appropriate wording: 'CONFIDENTIAL (i.e., the researcher will know, but will not disclose my identity)' or 'NON-CONFIDENTIAL (i.e., my identity will be revealed in study results)'}*.
- **I understand that** the data from this study *{please pick appropriate wording: 'will not be published' or 'may be published or reused freely for research purposes only'}*.

I HAVE CAREFULLY STUDIED THE ABOVE AND UNDERSTAND THIS AGREEMENT. I FREELY CONSENT AND VOLUNTARILY AGREE TO PARTICIPATE IN THIS EXPERIMENT.

NAME _____ SIGNATURE _____

If at any time you have questions about the proposed research or your rights as a research participant, please contact the project's Coordinator.

Participants should be given two copies of the present consent form – one to keep, and one to sign and return to the SURVANT Consortium.