This project has received funding from Horizon 2020, European Union's Framework Programme for Research and Innovation, under grant agreement No. 653355

DELIVERABLE D2.3

IMPACT ASSESSMENT OF FORENSOR AGAINST DAPPECL REQUIREMENTS [ABRIDGED VERSION]

WORK PACKAGE 2 DATA PROTECTION, PRIVACY, ETHICAL AND CRIMINAL LAW (DAPPECL) CONSTRAINS

FORENSOR Project

Grant Agreement No. 653355

Call H2020-FCT-2014-2015 "Fight against Crime and terrorism"

Topic FCT-05-2014 "Law enforcement capabilities topic 1: Develop novel monitoring systems and miniaturised sensors that improve Law Enforcement Agencies' evidence- gathering abilities"

Start date of the project: 1 September 2015

Duration of the project: 36 months

DISCLAIMER

This document contains material, which is the copyright of certain FORENSOR contractors, and may not be reproduced or copied without permission. All FORENSOR consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information. The reproduction of this document or of parts of it requires an agreement with the proprietor of that information. The document must be referenced if used in a publication.

The FORENSOR consortium consists of the following partners.

No.	Name	Short Name	Country
1	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	GR
2	JCP-CONNECT SAS	JCP-C	FR
3	STMICROELECTRONICS SRL	STM	IT
4	FONDAZIONE BRUNO KESSLER	FBK	IT
5	EMZA VISUAL SENSE LTD	EMZA	IL
6	SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION MONOPROSOPI EPE	SYNELIXIS	GR
7	VRIJE UNIVERSITEIT BRUSSEL	VUB	BE
8	ALMAVIVA - THE ITALIAN INNOVATION COMPANY SPA	ALMAVIVA	IT
9	VISIONWARE-SISTEMAS DE INFORMACAO SA	VISIONWARE	PT
10	VALENCIA LOCAL POLICE	PLV	ES
11	POLÍCIA JUDICIÁRIA (MINISTÉRIO DA JUSTIÇA)	MJ	PT

DOCUMENT INFORMATION

Project short name and number	FORENSOR (653355)
Work package	WP2
Number	D2.3
Title	Framework for impact assessment of FORENSOR against DaPPECL requirements
Responsible beneficiary	VUB
Involved beneficiaries	ALL PARTNERS
Type[1]	R
Dissemination level[2]	PU
Contractual date of delivery	31 August 2016
Last update	06/09/2016

[1] **Types. R:** Document, report (excluding the periodic and final reports); **DEM:** Demonstrator, pilot, prototype, plan designs; **DEC:** Websites, patents filing, press & media actions, videos, etc.; **OTHER:** Software, technical diagram, etc.

[2] **Dissemination levels. PU:** Public, fully open, e.g. web; **CO:** Confidential, restricted under conditions set out in Model Grant Agreement; **CI:** Classified, information as referred to in Commission Decision 2001/844/EC.

Document History

Version	Date	Status	Authors, Reviewers	Description
v 0.00	01/07/16	Template	VUB (P. Quinn, I. Böröcz, D. Kloza, P. De Hert)	Collecting the answers to the DaPPECL IA questionnaire
v 0.01	03/08/16	Template	VUB (P. Quinn, I. Böröcz, D. Kloza, P. De Hert)	First Draft
v 0.02	05/08/16	Draft	VUB (P. Quinn, I. Böröcz, D. Kloza)	Table of contents and document structure.
v 0.20	10/08/16	Draft	VUB (P. Quinn, I. Böröcz, D. Kloza)	Implementation of answers to the DaPPECL IA questionnaire
v 0.40	15/08/16	Draft	VUB (P. Quinn, I. Böröcz, D. Kloza)	Document ready for internal review
v 0.50	24/08/16	Draft	JCP-C (R. Kaurson, D. Yankova)	Additional information provided
v 0.60	25/08/16	Draft	VUB (P. Quinn, I. Böröcz, D. Kloza)	Finalizing the document
v 0.70	26/08/16	Draft	JCP-C (R. Kaurson, D. Yankova); VW (F. Custodio); ALMA (E. F. Becattini)	Additional comments
v 0.80	26/08/16	Draft	VUB (P. Quinn, I. Böröcz, D. Kloza)	Implementing the comments

v 0.90	29/08/16	Draft	All partners	Finalizing the document
v 1.00	31/08/16	Final	CERTH	Final document for submission
V 1.01	06/09/16	Final	VUB (P. Quinn, I. Böröcz, D. Kloza)	Abridged version excluding confidential information

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	**Description**
CIS	Contact Image Sensor
DaPPECL	Data Protection, Privacy, Ethics and Criminal Law
ECHR	European Convention on Human Rights
EDA	Event Driven Architecture
FORENSOR	FOREnsic evidence gathering autonomous seNSOR
GDPR	General Data Protection Regulation
IA	Impact Assessment
LEA	Law Enforcement Agency
SBA	Server Based Application
SECSOC	Security System on Chip
SOA	Service Object Architecture
SOC	System On Chip
VSN	Visual Sensor Network
WSN	Wireless Sensor Network

CONTENTS

LIST OF FIGURES

Figures do not appear in the abridged version.

LIST OF TABLES

Figures do not appear in the abridged version.

EXECUTIVE SUMMARY

The present deliverable contains the DaPPECL impact assessment report, i.e. the assessment of the impacts of the FORENSOR system and of the components thereof on data protection, privacy, ethics and criminal admissibility. The present report focuses on the whole FORENSOR system during project lifetime, furthermore it considers its effects on the individual as a commercial system as well. During project lifetime, the consortium will develop the prototype only, it will not be a commercial system. The introduction (Chapter 1) of the present deliverable discusses the approach of the FORENSOR project consortium to the DaPPECL IA as well as the description of the IA process actually carried out. Chapter 2 provides answers to the IA questionnaire (developed and revised in Deliverable D2.2). Chapter 3 contains the assessment of the identified, analysed and evaluated risks. Chapter 4 defines the selected risk treatment plans in order to avoid or minimize the possible negative consequences and impacts. Chapter 5 summarizes the recommendations and plans for effective risk treatment.

1. Introduction to the abridged version of the present deliverable

The present version of Deliverable 2.3 has been prepared in order to make public the results of the DaPPECL impact assessment process of the FORENSOR system. Since the original version of the said deliverable contains information that the project's partners consider confidential due to its technical and/or commercial nature. The dissemination level of its original version has been lowered from "public" to "restricted".

This document is based on the original text of the DaPPECL IA report as provided for in the full version of the Deliverable 2.3. The removed text has been marked [Confidential]. In certain situations, in order to make the abridged version meaningful, the removed text has been summarised; these sections are marked [Public summary].

1.1. Scope of the IA

Work package 2 of the FORENSOR project foresees the execution of an impact assessment on the risks the project poses on the individual in terms of data protection, privacy, ethics and matters related to the use of criminal evidence. Due to the use of the system, risks might occur during both the project and the commercial use. The key principles, that must be met in each of these areas, were presented in deliverable D2.1. This FORENSOR impact assessment occurred in two phases, each corresponding to Deliverable 2.2 and 2.3 respectively.

According to the Framework for impact assessment of FORENSOR against DaPPECL requirements (cf. Deliverable D2.2), any partner to the consortium that develops any element of the FORENSOR system, as well as the consortium as a whole with regard to the whole FORENSOR system, should carry out a tailored-down DaPPECL impact assessment by:

- providing answers to the questionnaire (presented in D2.2) for assessing the impact of the FORENSOR system and of the components thereof on data protection, privacy, ethics and matters related to the use of criminal evidence and
- applying the recommendations derived as an outcome of this process, before the component (subsystem, system) is finalized and deployed.

The same holds for when changes that have an impact on DaPPECL requirements are made to an element of the FORENSOR system. Due to the structure of the FORENSOR system that contains several technical and logical elements, i.e. high-level scene interpretation, development of a SBA or configuration of a microprocessor, and in order to fully assess their impact, the consortium developed a "small-scale" IA for these elements, de facto by "minimizing" the main model. On top of that, a "full-scale" IA has been performed for the system as such, since integration of all elements of the system might raise new ethical, privacy and data protection concerns or affect the applicability of the records as criminal evidence. Thus the "full-scale" IA pays special attention to examine interconnections and interactions between these elements. The present deliverable contains a "full-scale" DaPPECL IA, thus focusing on the separate elements by themselves along with their interconnections with each other whereas several questions target the impacts of the application of device as a whole. Deliverable D2.4, due in M18, and D2.5, due in M36 of the project, will contain a revision of the "full-scale" IA if necessary, as well as all "small-scale" IAs.

1.2. The process of DaPPECL IA in FORENSOR

Filling in the DaPPECL IA questionnaire has been a collaborative process. The technical partners divided labour among themselves and provided answers in several documents via email (closed to the public), separate from the questionnaire. These answers were subsequently edited by partners (without special technical expertise) and assembled into the present deliverable. The IA report contains original contributions from the technical partners with minor editions by the non-technical partners. From the practical viewpoint, the first draft of the framework has been extensively discussed and explained on a meeting with all partners (Valencia, 31 May – 1 June 2016) and non-technical partners have been available for subsequent consultations via e-mails and telcos. While drafting the framework as well as during the process of the DaPPECL IA, partners without technical expertise realised that the questions in the IA framework were not clear to the technical partners and, thus, some clarifications were needed. The most important problem was the poor understanding of ethical and legal terms by partners with technical expertise and – vice versa – of technical terms by partners without technical expertise.

1.3. Glossary

- EDA - There are architectures to offer services inside/outside a system (in case of FORENSOR the SBA), to organize and share information: EDA is the broker to lead messages in/out the system and orchestrates behaviour around the production and consumption of the events, and SOA allows the cooperation of the modules inside the SBA to organize, store, and retrieve information.
- Gateway - It is the FORENSOR node that connects the FORENSOR nodes which belong to wireless Visual Sensor Network (VSN) and the Server – based Application LEA through the Internet or intranet. In this sense the Gateway, provides two network interfaces (towards the VSN and the Internet / intranet) and can communicate with both networks. It is responsible

for transferring the information (alerts, evidence and commands) from one network to the other.

- High level algorithm - High Level Algorithms constitute the built-in intelligence of FORENSOR. They are responsible for object classification as well as for motion analysis and event detection.
- Identity Management module - defines the set of administrative functions such as identity creation, propagation, and maintenance/policies of user identity and privileges (user management, password management, role/group management and user/group provisioning or de-provisioning).
- SBA - SBA is the system that receives, stores, manages, and retrieves big data in compliance with a complex legal, ethical, privacy framework. The SBA receives and stores alert, video and picture sent by Gateway. The SBA allows the Users to manage the evidences gathered (using a Graphical User Interface), to help the LEA User with his investigations.
- SECSOC - The actual version of the SoC used for acquisition of data from the sensor, local data processing and management of transmission.
- SOA - There are architectures to offer services inside/outside a system, to organize and share information: EDA is the broker to lead messages in/out the system and orchestrates behaviour around the production and consumption of the events, and SOA allows the cooperation of the modules inside the SBA to organize, store, and retrieve information.
- SOC - It is an integrated circuit (IC) that integrates all components of a computer or other electronic system into a single chip.
- WSN - The nodes that compose the VSN can retrieve and store evidence, communicate with each other and with the Gateway. The alerts and the evidence can be sent to the Server Based Application. As visual data are retrieved, we also refer to it as wireless VSN.

2. Assessing the impact of the FORENSOR device and of the components thereof on the DaPPECL requirements

The method of the assessment follows the structure developed and introduced in chapter 1.2 and 1.3 of Deliverable 2.2. Present deliverable focuses on the *'assessment of the impacts of the activity'* (through the description of the project, identification, analysis and evaluation of risks) and on the '*evaluation and treatment of the assessed impacts and decision-making based on the findings, general objectives*'. The last step ('*monitoring and review')* will occur in Deliverable D2.4 and D2.5. This chapter contains the IA questions and the answers, provided by the consortium.

2.1. Technical description

1. Provide a brief overview of the element of the FORENSOR device you are developing.

FORENSOR is developing a novel, intelligent, autonomous, miniaturised, infrastructure-less and wireless visual sensor, with its supporting communication protocols and monitoring station, able to covertly acquire forensic evidence effectively and cost-effectively, while complying with all legal and ethical standards and regulations. Every system component is scalable both horizontally and vertically in order to ensure the possibility of modifications, additions. This concept is built up from separate elements and it is summarized below:

Hardware (for functioning and communication) /ST, FBK/: [Confidential]

Software for communication between components /JCP, VW/: [Confidential]

Communication between components /EMZA, CERTH/: [Confidential]

Communication between device and control centre /SYN, ALMAVIVA, VP, PJ/: [Confidential]

2. What are the functionalities of this element?

Hardware (for functioning and communication) /ST, FBK/: The microprocessor will receive the data from the FORENSOR video sensor, elaborate it understanding the scene and detecting the events included in the use cases. The processor will also prepare the alert signals associated with the events, and will prepare, store and transmit the data needed for forensic evidence.

[Confidential]

Software for communication between components /JCP, VW/: The communications block is responsible for the communications activities among the FORENSOR nodes and between the nodes and the Gateway. [Confidential]

Communication between components /EMZA, CERTH/: [Confidential]

Communication between device and control centre /SYN, ALMAVIVA, VP, PJ/: SBA should receive, store, manage and retrieve large amount of data (which were recorded beforehand). The SBA receives and stores alert, video and picture sent from the Gateway, to help the LEA user in investigations. [Confidential]

3. What is the need for this element? Would it be possible to substitute it with a different element?

Hardware (for functioning and communication) /ST, FBK/: The microprocessor consumes less power than usual microcontrollers, enabling the autonomy requirements of the FORENSOR use cases. [Confidential]

Software for communication between components /JCP, VW/: The communication block supports the interaction between the parts – related to the functionality of the node. [Confidential]. It is also noteworthy that the developed mechanisms can be applied to other wireless sensor networks where low power operation is required.

Communication between components /EMZA, CERTH/: The sensor and the low-level algorithms are basic and central elements of the system – [Confidential]

Communication between device and control centre /SYN, ALMAVIVA, VP, PJ/: The component of system application is essential to receive and to store alerts, videos and pictures sent from Gateway to allow LEA User in looking for and managing evidences correlated to his investigations. [Confidential]

4. What outcome (form of contribution to the whole system) is expected from the element?

Hardware (for functioning and communication) /ST, FBK/: The microcontroller will produce the alerts and the data needed for the forensic evidence. [Confidential]

Software for communication between components /JCP, VW/: The communication block will make the effective interaction between the parts possible. [Confidential]

Communication between components /EMZA, CERTH/: Acceptable performance of the chip is expected. [Confidential]

Communication between device and control centre /SYN, ALMAVIVA, VP, PJ/: [Confidential] The VSN and the SBA could be configured to transfer evidence to legal Courts for appropriate procedural uses, assuring the coherence, integrity and DaPPECL compliance.

5. What are the costs of the deployment of the element? Is there an option for cheaper solution with same effectiveness?

Hardware (for functioning and communication) /ST, FBK/: At the time of the impact assessment the microcontroller chip is not yet a product, therefore its actual cost could be only based on estimation. [Confidential].

Software for communication between components /JCP, VW/:

- *Deployment:* From the point of view of the Communications Block, [Confidential], the cost is similar to that of other relevant solutions.
- *Development:* The Communications Block consists of Hardware and Software. For the hardware [Confidential] the price is similar to that of other relevant products. [Confidential] Regarding the software part, free solutions are leveraged, upon which custom software is being built. Otherwise no information by nature of question assumes commercial usage of the mechanism. So far, the project is in development stage.

Communication between components /EMZA, CERTH/: High-level Scene Interpretation is a software being developed following the strict power budget constraints associated with an autonomous sensor. [Confidential]

Communication between device and control centre /SYN, ALMAVIVA, VP, PJ/: The deployment of the element aims to remain cost efficient. [Confidential]

For the control enter (LEAs) the most economic-friendly option will be that requiring less personal intervention for the realization of most economic objective.

6. Is the effectiveness of the component/system regularly evaluated? If so how?

The effectiveness of the components is evaluated during the definition of the architecture of the system, and a successive change could be very hard, arduous and expensive. It will be possible that next improvements or extensions of the whole system in the time will occur (in accord with the market needs).

2.2. Data Protection

7. **What types of data will be collected? Are the participants able identify a natural person with the collected data (in itself or combined with other data, such as criminal records)?**

Hardware (for functioning and communication) /ST, FBK/: The data collected by the microcontroller will be:

- Compressed images related to a specific event;
- Results of video analysis [Confidential].

Software for communication between components /JCP, VW/: The Communications Block is not aware of the actual data (alert and evidence) that is being transferred. It transfers the data as instructed by the High Level Algorithm. [Confidential]

Communication between components /EMZA, CERTH/: The sensor will be able to acquire images with enough resolution to identify persons. [Confidential]

Communication between device and control centre /SYN, ALMAVIVA, VP, PJ/: The types of data collected could be personal data, however not always will it be possible to identify a natural person. [Confidential]

8. **Do you process special categories of data (such as data concerning health)?**

Although the consortium does not explicitly capture or process special categories of data, some accidental processing, however unlikely, is possible. [Confidential]

9. **Does the component/system process meta-data? If yes, what kind of meta-data?**

Metadata are data providing information about one or more aspects of data related to an evidence; it is used to summarize basic information about those data, which can make tracking and working with specific data easier. [Confidential]

10. **What is the collected data used for?**

FORENSOR aims to create a platform that will gather and deliver evidence for criminal prosecution that will be accepted in a court of law. [Confidential]

11. **Does the collected data meet the requirements of relevancy and accuracy? How do you ensure that data will remain accurate when disclosing it to third parties (e.g. to a prosecutor)?**

The collected data intends to meet the requirement of relevancy to a greater extent than in conventional surveillance systems through a set of technical controls. [Confidential]

12. **Would you be able to estimate the amount of processed data and the number of data subjects?**

The amount of data depends on the specific requirements of application and the use case which is not defined yet (M12). There will be a lot of locally obtained data, and whatever datasets collected by the consortium. In any case they will be defined for the satisfaction of user (LEAs) requirements. [Confidential]

After the project, in case of criminal investigations a decision must be done by a judge on the impact on privacy of citizens versus the justification for the criminal investigation prior to the deployment of the device. This decision must include the lifetime of the surveillance. All images that are not usable for the criminal investigation are destroyed as soon as possible.

13. Who has responsibility for control of the processed personal data and who decided how can it be used? Who determines the means and details of the processing operations?

During the project lifetime the data controller of the FORENSOR project is Prof. Paul De Hert. After the end of the project – in a typical use case – it will be the respective official of the police force using the system under the supervision of the respective prosecutor (according to the legal provisions of the country where the system will be used). However, this also depends on by whom the system will be used (e.g. the final product might be also sold to other types of organisations and for different applications).

[Confidential]

14. Would an organizational change (either in consortium or in single organisation) affect the data processing in any sort of way?

Not really. At least not if the data controller and/or data processor roles are reassigned in time. The profiles and grants to access at data in FORENSOR will not change in case of an organizational change, unless there is a change in profile settings. [Confidential]

15. Will the data be transferred to third countries? If yes, does the third country provide adequate protection? What is the legal ground of the transfer?

It is possible to transfer data to third countries based on international cooperation framework protection of such data that will be covered by international agreements between attorneys and LEAs in other countries. Data downloaded from FORENSOR system will be wrapped with layers of security, encryption, and digital signature in order to preserve integrity. Otherwise LEAs have no intention to transfer data to any individual or institution other than the judicial authority for legal purpose evidence, it should be requested and authorized by a judge.

16. How do you demonstrate compliance with data protection law?

Compliance with the data protection law is demonstrated in at least the following ways:

- An Impact Assessment has been conducted (present and forthcoming deliverables by WP2 – D2.4 (M18) and D2.5 (M36));
- The DPAs will be properly notified (according to the national laws) regarding the project's Development and Testing Benchmark;
- The FORENSOR Development and Testing Benchmark is being kept safely (password protected, access allowed to authorised employees only, tagged files, properly organisation of files, proper filenames etc.) at the premises of CERTH;
- All software used for the processing of the FORENSOR Development and Testing Benchmark is properly documented;
- All processing actions on the FORENSOR Development and Testing Benchmark are properly logged;
- The data is encrypted in the device. [Confidential]
- The requirements of the FORENSOR WSN and SBA are compliant with national regulations relating to the processing of personal data;
- Appropriate signage will be put in places where the sensor will be installed and the persons involved in the test movies will sign a specific authorization

17. **Please introduce the functioning the FORENSOR device component by component (for non-specialists, with special attention to the method of data processing and the tools to be used)!**

[Confidential].

18. How do you inform the data subjects about the intended data processing operation (what is the content and the used platform)? Please describe methods to be used to provide information to the data subjects!

Data subjects before the initiation of the testing phase sign a consent form before the start of any data processing operation. Data subjects are informed about the intended data processing operation through:

- the consent form they sign prior to any participation, which is informing them about all the relevant details;
- appropriate signs at the entrance points of the areas where cameras are positioned are also used (for bypassers) as it is mandatory;[3]
- where necessary to ensure the full right of information to people, in relation to the vastness of the area subject of survey, to the number of cameras and the shooting mode, there will be installed more signs;
- further information will available on the website under a separate tab/subpage (http://forensor-project.eu/).

19. What is the legal ground and the purpose of the data processing? What are the expected benefits of the processing?

[From the perspective of research conducted during the FORENSOR project] Processing of personal data will be based on the consent of the data subject.

[From the perspective of use of a FORENSOR device in a criminal investigation] After the project, the FORENSOR-based product will be used in lawful surveillance of subjects in criminal investigations. The legal ground is established by the judicial authorities that authorize the surveillance (otherwise - in case of private use - the provisions of data protection law should apply).

The expected benefits are the following:

- To increase the efficiency of evidence gathering and covert surveillance in areas where regular CCTV camera is hard or impossible to be deployed,
- To guarantee and protect the right to honour, to privacy and to right to one's own image,
- Further benefits are described in the DOW.

20. If the processing of personal data will be based on the consent of the data subject, how do you guarantee that it was informed, specific and freely given?

[3] [Confidential]

Informed, specific and freely given consent is guaranteed through the signing (by adults mentally and physically able to give consent), [Confidential]

21. Is the end date of the processing set (how long is the personal data retained)? What will happen with the personal data afterwards? Please answer from the perspective of both research conducted during the FORENSOR project and the use of a FORENSOR device in a criminal investigation.

The expected end date of the processing is one month after the official end date of the FORENSOR project (which is 31 August 2018). Personal data will be retained either until one month after the finalisation of the FORENSOR project (30 September 2018) or until the end of the retention period specified by the laws of the country where the investigation will take place, whichever comes first (the start of the retention period depends on the time of the first data processing activity – most likely recording).

[Confidential]

After that, the personal data will be either properly destroyed (and a proof of destruction will be kept) or, in case the data are going to be used further for research purposes, they will be dully anonymised (blurring of all faces depicted).

[Confidential]In case of the records will be used in a criminal procedure, they should be validated by a judge. Then, what is useful to the investigation goes to the investigation file, and the rest is destroyed.

22. What Privacy Enhancing Technologies (PETs) are used?

Anonymization in the form of blurring of faces or car plates might be used, furthermore communication can be encrypted. Other PETs are to be defined in the S&D Integration workgroup.

23. How do you ensure the security of data? Please explain!

The collected data will be locally encrypted [Confidential], guaranteeing that the data cannot be read or modified by non-authorized persons. Access to the FORENSOR nodes is authenticated and authorized. [Confidential]

24. Is the access to the personal data restricted? What are the rules of access (with special attention to its conditions, mode, and limits)?

The access to the FORENSOR node, through the wireless network, is authenticated and authorized. [Confidential]

25. Are the processing operations documented? How are the records maintained?

[Confidential] Yes, there are logs of every access and every action on the data. [Confidential]

26. How do you ensure for data subjects to use their rights? Please answer from the perspective of both research conducted during the FORENSOR project and the use of a FORENSOR device in a criminal investigation.

[From the perspective of research conducted during the FORENSOR project] During the period of project development people involved in the videos captured for test will be informed about the use of their personal data and will give their authorization to their use. As part of the information every data subject is given the contact details of the FORENSOR Data Controller and the respective project partner, therefore they will be able to address their will of practicing their rights. The FORENSOR consortium guarantees that requests of data subjects will be addressed immediately.

[From the perspective of use of a FORENSOR device in a criminal investigation] Depending on the end user of the system (e.g. police or other type of organisation) the addressee of requests of data subjects can be either the chief-officer of the police department, the prosecutor or the data controller. They should be responsible to ensure the use of the rights of data subjects.

27. How do you provide information to the data subject about the processing operation of FORENSOR? What is the content of the notice? Please answer from the perspective of both research conducted during the FORENSOR project and the use of a FORENSOR device in a criminal investigation.

[From the perspective of research conducted during the FORENSOR project]

During the period of project development, the people involved in the videos captured for test will be informed about the use of the data and will give their authorization to their use.

- Information about the processing operation of FORENSOR is provided to the data subject through referral to the project website (www.forensor-project.eu).
- The content of the notice contains at least the following:
    - Project details and overview
    - Project Consortium overview and contact details
    - Project Overall Concept, Use Cases, and User Requirements
- Public deliverables of the project
- News, newsletter and publications
- It must be emphasized that the FORENSOR website will be active for at least two years after the end of the project.

[From the perspective of use of a FORENSOR device in a criminal investigation]

It will depend on the regulation of the end-user organization, but in general it includes to put information panels, signs, in the location of the video surveillance in advance, to explain the start of the processing of personal data, the activation of video surveillance, any increase in size of the video setup and on any subsequent ending for any cause of data processing performed. Data processing for prevention purposes, detection and crime suppression and for urban security purposes could not be provided in accordance with the data protection framework as well as in cases where specific reasons of investigation and public safety shall be without prejudice, if information does not allow undertaking of specific functions pursued. The guarantee of the information given to the person involved in a crime resides in the fact that the individual understands the situation and his rights in the criminal investigation.

28. Would the use of a layered notification system help the individuals to gain more information and understand the necessity of the FORENSOR device?

A layered notification system is already used as described in the answer to question 26 above.

29. Are data subjects involved to the development phase? If yes, on what extent?

Yes, data subjects are involved during the development phase. Besides their involvement in data capturing they are also consortium members of the user partners, which means that they are involved in the system design as system stakeholders. However, no involvement of subjects external to the FORENSOR consortium to the development phase is foreseen, except the possibility to contact the FORENSOR consortium through the project website.

30. How do you plan to collect the views and feedbacks of stakeholders?

The views and feedbacks of internal stakeholders are being collected through various ways, including:

- Emails;
- Providing demonstrations of the capabilities of the entire system or intermediate prototypes;
- Provide performance metrics as part of the consortium meetings and deliverables;
- Meetings (including telephone conference and physical meetings).

The details are described in detail in D3.1 “Use case analysis and user scenarios” of the FORENSOR project. Additionally, task 8.3 foresees a survey that will collect feedbacks from stakeholders. The task will analyse the pilot results obtained in previous tasks. The results will undergo a thorough comparative evaluation, including technical, usability, strategic, sensitivity and socio-economic analysis. Sensitivity analysis will identify the key parameters of user acceptance.

31. Will the personal data, processed by FORENSOR, be used in cross-border cooperation by police authorities?

During the research phase of FORENSOR system the data will be shared only between consortium partners. Otherwise the only addressee of LEAs is the judicial authority, thus they cannot make any other use with the information obtained. Requests from abroad to access to data will be denied.

32. Is it possible that, if it is absolutely necessary, the FORENSOR device will be applied and used without informing the data subjects? If yes, what safeguards or security measures would be applied?

Without the cases specifically mentioned, minimum disclosures will be provided even if the treatment is carried out for prevention purposes, investigation and prosecution of criminal offenses and for urban security purposes. The 'absolute necessity' parameter can't be considered by LEAs but by the judicial authorities.

2.3. Privacy

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

- **[No impact] Bodily privacy:** It relates to the physical body and its physical privacy, linked to physiological and safety-related needs. Examples include physical and unsolicited harms to the body.
- **[Impact] Spatial privacy:** Physical or spatial privacy refers to the privacy expectations in and around one's home, as a general example, however it may be extended beyond the intimate zone. In FORENSOR the video record will include GPS stamp thus the location of a person can be extracted, affecting his or her privacy.
- **[No impact] Communicational privacy:** A person's interest in restricting access to communications or controlling the use of information communicated to third-parties. FORENSOR system does not record, process or in any other way deal directly with personal communication data.
- **[No impact] Proprietary privacy:** It relates to reputation and is similar to "the right to one's honour". Typified by a person's interest in using property as a means to shield activity, facts, things, or information from the view of others. As the FORENSOR sensor will not be able to record activities covered by different objects (by e.g. heat sensor), there will be no impact on proprietary privacy.
- **[Impact] Intellectual privacy:** It describes the interest in privacy of thought and mind, and the development of opinions and beliefs. [Confidential]
- **[Impact] Decisional privacy:** It is typified by intimate decisions, primarily of a sexual or procreative nature, but also including other decision-making on sensitive topics within the context of intimate relationships. As with spatial privacy, decisional privacy as an ideal type within the intimate zone is closely related to family life. [Confidential]
- **[Impact] Associational privacy:** It includes values and criteria for inclusion and exclusion. It describes individuals' interests in being free to choose who they want to interact with: friends, associations, groups, and communities. [Confidential]
- **[Impact] Behavioural privacy:** It covers type or set of personal actions and behaviours that should remain private, even in public places. It covers the privacy interests a person has while conducting publicly visible activities. One's personal behaviour in public spaces is more difficult to exclude others from observing, and thus is an ideal type of privacy where the need for control after access has been granted is most pressing. FORENSOR will record activities in public places therefore the protection of those records are crucial.

- **[Impact] Informational privacy:** Informational privacy is an overarching aspect of each aforementioned type, described by the individual need in preventing information about one-self to be collected and in controlling information about one-self that others have legitimate access to. FORENSOR, through its functional characteristics, will affect informational privacy.[4]

34. Does the FORENSOR device and its functionality meet the requirement of proportionality? Is it necessary in a democratic society?

Surveillance and particularly video surveillance is a tool applied by LEAs in democratic societies in order to increase their efficiency against dangerous forms of illegal, antisocial and violent activity or even novel and extremely destructive types of attacks (e.g. individual or group acts of terrorism). Video surveillance is a tool that poses issues regarding the privacy of the individual but, at the same time, provides benefits regarding the security, safety and peaceful living of citizens in a democratic society. Thus, surveillance in general and video surveillance in particular should fulfil the principle of necessity and proportionality by achieving a balance between the two fundamental rights:

- The Right to Privacy. *"The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose."*[5]
- The Right to Life. *"Everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which this penalty is provided by law. Deprivation of life shall not be regarded as inflicted in contravention of this Article when it results from the use of force which is no more than absolutely necessary:*
    - *(a) in defence of any person from unlawful violence;*
    - *(b) in order to effect a lawful arrest or to prevent the escape of a person lawfully detained;*
    - *(c) in action lawfully taken for the purpose of quelling a riot or insurrection."*[6]

The inadequacy and inefficiency of the existing surveillance systems shifted the balance between the two aforementioned fundamental rights against the right to life. FORENSOR is aspiring to help restore

[4] This typology of privacy was based on: Koops B J, Newell B C, Timan T, Škorvánek I, Chokrevski T and Galič M, 'A Typology of Privacy' In University of Pennsylvania Journal of International Law, Forthcoming http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043 [19/06/2016]

[5] Yael Onn, et al., Privacy in the Digital Environment , Haifa Center of Law & Technology, (2005) 1-12

[6] ECHR art. 2

the proper balance between those two fundamental rights by providing to LEAs a state-of-the-art tool that will make video surveillance both adequate and efficient again.

35. Does the use case scenario represent a situation where the use of a FORENSOR prototype would be justified?

[Confidential]

[Confidential] This selected use cases have severe adverse effects on the overall population of Europe, and thus justifies the usage of advanced surveillance techniques under the proper legal framework to investigate these illegal activities.

36. Are there situations outside the use case scenarios where the use of a FORENSOR prototype would be necessary?

Only the required situations those related to the investigating competence of LEAs within the criminal field were considered. [Confidential] The question will be addressed by WP9 (exploitation activities, described in D9.8 and D9.9 due to month 26 and 36).

37. Are there procedures within your operating experience for determining the necessity (in legal terms) of surveillance practices and would a FORENSOR prototype fit within such contexts?

Yes, CCTV cameras are used by the involved LEAs, and the application of the FORENSOR device would not require different procedure. [Confidential] The usage of the FORENSOR device will fall into the same category as all other surveillance methods the police has to monitor, investigate and prosecute criminal activity, meaning that the proper procedures and rules, framed by strict legal constraints designed to protect the citizen from undue prosecution and unreasonable intrusion into the individual's rights, are already in place.

38. Will faces be visible? If so under what conditions?

Yes, the faces will be visible ([Confidential]) depending on the position of the camera respect to the persons, but in general it cannot be excluded. Regarding the conditions: [Confidential].

39. Can car number plates be identified? If so under what conditions?

Yes, [Confidential].

40. Is there a possibility to mask faces so that they are not visible?

It is possible to implement face detection algorithms and obscure that portions of the image, [Confidential]

41. Is unused data deleted automatically? If so how soon/how often does this occur?

Unused data are not stored at all due to severe storage space restrictions in the FORENSOR (sensor), it will be transferred immediately. [Confidential]

42. Who will have access to the data in question?

Only authorized persons with specific profile with grants to access FORENSOR SBA.

43. Can the features described in questions 38-42 be programmed on a case by case basis?

The described features could be programmed on a case by case basis [Confidential]

44. Can the algorithms for activation of recording be altered simply (i.e. by the police using the device)?

No, the embedded system does not allow access to this functionality. The FORENSOR sensor is an embedded system and reprogramming of the system will be needed to alter the alerting mechanisms of the system. [Confidential]

45. If not who has the ability to alter the algorithms for detection and activation?

The qualified technical staff: programmers and specialized agents trained to do so.

46. Is the stored data secure from unintentional/malevolent access?

The intention is to be secure - one of the objective of FORENSOR is to secure stored data from non-authorized access. Various technologies and processes are used to ensure this. [Confidential]

47. Will it be a simple matter to alter the detection algorithms of the FORENSOR prototype or a difficult and time consuming task? Will the alteration of a detection algorithm require prolonged contact between LEAs and technical staff?

There are very simple parameters that are designed for easy configuration. Any other adaptation would be very difficult and time consuming since reprogramming of the sensor will be needed, furthermore direct access to the sensor would be required. Thus the contact would be definitely prolonged.

48. Will those performing alteration of the technical algorithm have to be familiar with the deployment site in question?

Not necessarily specific scene itself but it depends on the requirements set out by the end-users.

49. Are the detection algorithms likely to be flexible enough to meet the potential varying specifications of an investigative judge or magistrate that may be in charge of approving warrants for the use of surveillance devices by the police?

They should be. This is a requirement for the FORENSOR sensor.

50. Are the detection algorithms used in a particular device likely to be comprehensible to police figures, investigating judges and magistrates?

Yes, [Confidential].

2.4. Ethics

51. What ethical issues can this component/system raise? What harm might the FORENSOR component/system cause to the individual?

The ethical issues relevant to the FORENSOR project concern primarily individuals recorded by the FORENSOR device and identifiable either directly or indirectly through reference to individuals. The second category of ethical issues in the FORENSOR project consists of an impact thereof on the society as a whole. If the FORENSOR system is deployed and adopted for operation, it could cause harm to the individual regarding his or her privacy; this includes any side effects that such harm could cause.

52. What potential benefits will the FORENSOR component/system bring to the individual?

The FORENSOR system and its components are carefully designed to help LEAs in covert video surveillance while protecting people's privacy and personal data as well as observing ethical principles. The system is designed in a way that compensates the abovementioned possible harm with the ability to improve crime investigation and provide safer public spaces to the community and thus, indirectly, all individuals. Bringing this efficient technology into the process of investigation would benefit from increased chances to decrease the level and amount of crimes.

53. What threats to society does the FORENSOR component/system address? How is it appropriate to address these threats?

FORENSOR develops an intelligent, wireless and autonomous video sensor, with real-time scene interpretation analytics and recording capacities for use by LEAs for crime detection and evidence gathering purposes. Thus, the research aims to foster the fight against crime (including the organised crime such as the illegal drugs dealing), detection and prevention of potentially dangerous events (e.g. street racing). FORENSOR is expected to have a positive impact on society on the level of security, resulting in a safer and carefree everyday life.

54. How will society as a whole benefit from the FORENSOR component/system? What segments of society will benefit?

The research addresses the protection of a number of documented societal needs, such as life, health or property, by enabling LEAs' prompt reaction to dangerous events and more efficient prosecution of crime. Improving the efficiency of LEAs also strengthens the feeling of justice and security safeguarding the societal cohesion and values. FORENSOR surveillance technology, by supporting LEAs in their fight against crime, will be beneficial for all parts of society. More specifically:

- The morale of the citizens and their faith into societal and moral values and especially justice will be reinforced through the increased effectiveness of detecting crime, evidence gathering and effective crime persecution.

- Law Enforcement Agencies will find a valuable and socially acceptable ally in their work against crime, which can support them to improve their processes and methodologies.
- The stakeholders in the justice system will benefit from the availability of digital evidence.

2.5. Admissibility of criminal evidence

55. What are the procedures in your jurisdiction for approving the use of surveillance measures? Can records be used from surveillance as evidence in criminal proceedings in case the aforementioned procedures are not complied with?

Usually the national police act contains such provisions. For example, in Italy the video can be acquired in accordance with art. 234 Criminal Procedure Code and usable in court because it was considered as a document. In Portugal, according to the Criminal Procedure Code art 189)[7] The judge authorizes in strict compliance with the laws and the police performs. Records would not be used as evidence must originate from a legal source, thus non-compliant recordings would be rejected by the judicial authority.

56. If (in your jurisdiction) evidence is obtained during another investigation, can it be used for other criminal proceedings for which the original permission for the use of surveillance procedure had been granted?

- Italy – Yes, as long as legal rules are respected;
- Spain – Yes, as long as legal formalities are met and the judicial authority ultimately says so;
- Portugal – Yes, as long as legal formalities are met and the judicial authority ultimately says so. According to the Criminal Procedure Code (art. 189), the judge authorizes in strict compliance with the laws and the police executes the capturing of evidence.

57. Are there rules about the minimum image/video quality that can be used by surveillance processes in criminal investigations? Is there a threshold (in terms of quality) for the use of images or videos in court or can courts use their discretion?

- Italy - No, there are no such rules. Article 234 of the Code of Criminal Procedure which, in paragraph 1, allows "the acquisition of writings or other documents representing facts, persons or property by means of photography, cinematography, phonography or

[7] Section 189 Extension (1) - The provisions in sections 187 and 188 apply correspondingly to conversations or communications transmitted by any technical means other than the telephone, namely electronic mail or other ways of telematics data transmission, even when kept on digital equipment, as well as to the interception of communications between people present. (2) - The gathering and adding to the case file of data regarding cell location or of records regarding conversations or communications can only be ordered or authorized, at any stage of the proceedings, following a judicial order with regard to the offences provided for in subsection 1 of section 187 and concerning the persons mentioned in subsection 4 of said section.

any other means". In criminal proceedings the important aspect is to be able to identify useful facts, actions or behaviours in the images to fill an accusation.

- Spain – No, there are no such rules. In criminal proceedings the important aspect is to be able to identify useful facts, actions or behaviours in the images to fill an accusation.
- Portugal – No, there are no such rules. In criminal proceedings the important aspect is to be able to identify useful facts, actions or behaviours in the images to fill an accusation.

58. If a quality threshold exists is it different with regards to procedures relating to different types of offences?

- Italy – The Italian criminal and procedural law do not make any distinction between the different types of offences;
- Spain – The Spanish criminal and procedural law do not make any distinction between the different types of offences;
- Portugal – The Portuguese criminal and procedural law do not make any distinction between the different types of offences.

Generally, images must provide enough information to be considered as evidence.

59. Will the images and videos be time stamped? If yes, who sets the time stamp?

Yes, [Confidential].

60. Is there a technical difficulty to set the time stamp?

It depends on the availability of this information, but generally no.

61. Can such time stamps be altered?

Theoretically yes, but not legally and with a considerable amount of effort from the one that wants to alter the timestamp. [Confidential]

62. Will there be GPS 'stamp'? If so who would set the GPS 'stamp'?

Yes, there will be. The GPS location will be set by the FORENSOR sensor upon recording of the evidence. [Confidential]

63. Would it be difficult to alter the GPS stamp?

It cannot be modified in the platform, it is retrieved automatically and assigned to the given images or events in the video processing applications inside the platform. [Confidential]

64. Is there a way to stamp video evidence to show chain of custody?

Yes. This is one of the requirements of the FORENSOR sensor. [Confidential]

65. Will it be possible for instigating police to add to this chain of 'custody stamp'?

Yes, any action that guarantee the safety and avoid the tampering of evidences will result in a further procedural guarantee.

66. If there is no chain of custody stamp in the meta data what other methods will be used to demonstrate a valid chain of custody?

That the original recording support avoids the tampering.

67. Is it possible to retrospectively alter or tamper with video evidence? What precautions are taken against this?

Yes, but not legally and with a considerable amount of effort from the one that wants to alter or tamper the video evidence. This could be the case if significant part of the infrastructure is compromised. The images stored in the SBA will be protected against alterations, to preserve their integrity.
Regarding precautions:
[Confidential] will be applied. [Confidential] Any modification can be detected.

68. How will images and videos be viewed by investigating police and courts?

This is one of the goal of SBA, [Confidential]. Generally, the FORENSOR sensor will provide a specific format that cannot be altered. [Confidential]

69. Is it possible that images and videos are viewed differently?

They could differ but it would be inconvenient because of the lack of the criteria. [Confidential]

70. Can processes be applied to order to make images and videos clearer? If so are such processes standardized, reversible and repeatable in a transparent manner?

Yes, but always to a reasonable extent, however there is a large range of operations to improve video footage. Many of these are very well known and easy to explain or to demonstrate. Mostly they are standardized and repeatable, others are also reversible, but not all (for example an image can be smoothed by averaging adjacent pixels; this is irreversible). [Confidential]

71. If such processes exist are they used at present in court proceedings in the jurisdiction that you have knowledge of?

We know of no standard process, each evidence is treated in a case-by-case method, under the criteria of the person in charge to judge the evidence.

72. Will it be possible to present defendants with copies of images or videos that may be used against them in legal proceedings?

Yes, it will be possible within the right of defence of the defendant.

73. Will it be possible to explain and demonstrate any processes that have been applied to defendants and their legal counsel?

Yes, at least to some extent by the qualified technical staff as specialists in the area. It largely depends on how deeply experts want to go and what is the level of technical knowledge defendants and their legal counsel.

3. DaPPECL Risk assessment

The term ‘risk’ is usually used in the context of an adverse consequence of an event, however it is not necessarily a negative term: *„risk is the probability of an event multiplied by some measure of its consequence.”*[8] Risk analysis focuses on the understanding of the identified risk, by measuring the probability of occurrence and the weight of the possible consequences. The analysis can be based on different scaling systems[9], which depend on the type of risk, its possible consequences or the purpose of the analysis.[10] Generally the analysis is based on two factors of the risk: the probability of its occurrence and the weight of its impact.

As described in D1.3, **probability** of risk to occur can be rated to one of the following four scale:

- **Very unlikely** – Risk nature is known to FORENSOR partners and no known occurrences of the risk happened in similar activities. Risk shall be **periodically monitored**.
- **Rather unlikely** – Few occurrences of the risk happened in similar activities, thus risk can be handled relatively reliably. Threat or failure is possible and high-level action plan in case risk occurs should be elaborated. Depending on the nature or root cause, set **of preventive or mitigation actions should be identified**.
- **Reasonably possible** – Risks of similar nature has happened rarely in other similar activities and current situation has few assumptions that are somewhat favourable to occurrence of the risk. Detailed action plan in case risks occur should be developed. Depending on the nature or root cause, set of preventive or **mitigation actions should be assessed and broke down into steps**.
- **Likely** – The situation is favourable to occurrence of risks and/or similar risks happened in similar activities before. Major trade-offs between DaPPECL requirements and FORENSOR sensor functionalities should be thoroughly discussed and set of preventive or **mitigation actions** (depending on the nature or root cause) **should be ready to be triggered**.

The **weight** of the risk to the fundamental rights and freedoms of the individual should be properly assessed. Three scales of impact are assigned as follows:

[8] Gary Yohe and Robin Leichenko, ’Chapter 2: Adopting a risk-based approach’ (2010) New York City Panel on Climate Change 2010 Report, Annals of the New York Academy of Sciences 29,31 <http://onlinelibrary.wiley.com/doi/10.1111/j.1749-6632.2009.05310.x/epdf> [07/05/2016]

[9] Such as qualitative, semi-quantitative or quantitative. Read more at: ISO 31000:2009 5.4.3

[10] ISO 31000:2009 5.4.3

- **Low** - In case of occurrence, the risk doesn't threaten the rights and freedoms of the individual, or causes necessity of only minor adaptation of the project. Limitation of the DaPPECL requirements remains **lawful, necessary and proportionate**;
- **Moderate** - In case of occurrence, **risk can be deemed as a threat** to the rights and freedoms of the individual. Several elements in the system should be revised and/or modified (however stay on acceptable level);
- **High** - In case of risk occurrence, rights and freedoms of the individual are **highly threatened**, thus one or more goals of the project will not be met. Significant revision and re-orientation (e.g. technical) is needed.

In case of data protection related risks, the impacts will be qualified by a two-grade scale:[11]

- **Compliant -** The limitation of the right to the protection of personal data complies with data protection law;
- **Non-compliant -** The limitation of the right to the protection of personal data does not comply with data protection law.

To describe the **significance** of the identified risk the qualified weight and occurrence will be quantified and placed in a matrix:

		Probability			
		Very unlikely (1)	Rather unlikely (2)	Reasonably possible (3)	Likely (4)
Weight	Low (1)	1	2	3	4
	Moderate (2)	2	4	6	8
	High (3)	3	6	9	12

[11] A limitation of a right in itself is usually not quantifiable (or qualifiable), therefore the severity of risk should be described in a two-grade scale: the processing of personal data is either compliant or non-compliant. To analyse the nature of the severity the data controller must find out, whether the processing operation is in compliance with data protection law. Although the analysis of risk is not regulated by the GDPR, the severity of the risk can be measured, based on the governing principles of data protection law, the opinions of the Article 29 Data Protection Working Party and the national supervisory authorities.

The **significance** of risk will be divided into three categories, based on the quantified risk:

- **Low**: 1-4
- **Moderate**: 5-8
- **High**: 9-12

These categories will help the consortium to prioritize between risks and decide, which risks should be mitigated first and which leave space for other treatment options. The answers provided to the questionnaire contain enough information to identify, assess and categorize the probability and weight of risks against DaPPECL requirements. In case of the data protection risks the matrix will not be applicable as risks must be mitigated or avoided when data processing operation is not compliant with the legal provisions.

3.1. Technical risks

The identified and assessed technical risks refer to the final outcome of the project and presumes that every task will be completed and issues will be solved. Technical risks which might occur during the project are assessed in Deliverable 1.3.

[Public summary]: the DaPPECL IA has found 6 technical risk and defined their probability, weight and significance.

3.2. Risks related to data protection

[Public summary]: the DaPPECL IA has found 12 data protection risk and defined their probability, weight and significance.

3.3. Risks related to privacy

[Public summary]: the DaPPECL IA has found 8 privacy risk and defined their probability, weight and significance

3.4. Risks related to ethics

[Public summary]: the DaPPECL IA has found 9 ethical risk and defined their probability, weight and significance.

3.5. Risks related to criminal admissibility

[Public summary]: the DaPPECL IA has found 4 risk relating to criminal admissibility and defined their probability, weight and significance.

4. Risk treatment

There are four main strategies that can be used for negative risks identified in the project:

- **Avoid:** When you avoid the risk it means you change your plan to completely eliminate the probability of the risk occurring or the effect of the risk if it does occur;
- **Transfer:** Risk transference occurs when the negative impact is shifted to a third party, such as through an insurance policy or penalty clause in a contract. The risk may still occur however the financial impact will be somewhat displaced. Risk transference usually involves some type of contractual agreement;
- **Mitigate:** Risk mitigation occurs when you proactively change the plan to minimize the impact or probability of the risk occurring. Risk mitigation does not eliminate the risk and as such there will be some residual risk remaining;
- **Accept:** There are few risks which are out of control of project organization and project manager has no other option but to accept them and still continue running the project by finding alternate ways to tackle the issues arising from these risks.

This chapter will describe the identified risks, the selected risk response plan type (described above), the plan and reasons why the selected plan can be considered as the best in terms of efficiency, time, initial goals of the project, protecting DaPPECL requirements, etc. Some risks are already considered and treated. They will be indicated.

[Public summary]: The consortium decided which risk response type and risk response plan should be chosen to appropriately treat the identified risk. In most cases the response to the identified risks were the application of mitigating measures (27 out of 39). A significant number of them were already taken (14) which shows the competency and preparedness of the consortium. 7 risks were accepted, and 5 transferred.

5. Summary of recommendations

Based on the current outcomes of the DaPPECL IA, the consortium should consider the treatment of the identified risks and carry out the advised activities, with special attention to the applied mitigating measures and to the following:

[Public summary]: From a practical point of view the IA recommended, among others, the following:

- New technologies should be monitored, therefore new hardware and software modules could be added or updated in the future versions of the products to respect new requirements in terms data storage protection.
- Several technical aspects should be considered.
- The consortium should consider DaPPECL requirements throughout the whole project.
- Additional tools should be used to demonstrate compliance with data protection rules (e.g. involvement of external stakeholders).
- Certain risks should be emphasized when providing the system to other users after the project.

6. ANNEXES

6.1. Annex I –Impact assessment table

[Confidential