



*This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607881*

# ***Petty cRiminality diminution through sEarch and Analysis in multi-source video Capturing and archiving plaTform***



**Instrument:** Research and Innovation Action  
**Thematic Priority:** FP7- SEC - 2013.7.2-1  
**Grant Agreement:** 607881

## D1.6 – Guidelines for Ethical, Privacy and Data Protection Issues

<b>Deliverable Number</b>	D1.6
<b>Title</b>	Guidelines for Ethical, Privacy and Data Protection Issues
<b>Version</b>	2.1
<b>Date</b>	January 2015
<b>Status</b>	Final Version
<b>Dissemination Level</b>	PU (Public)
<b>Nature</b>	Report

### EC Distribution

**Project Partners:** Vicomtech-IK4 (VICOM); Kinesense (KS); Aditess (ADI); Future Intelligence (FINT); Center for Research and Technology Hellas (CERTH); Center for Security Studies (KEMEA); Societa Reti e Mobilita (SRM)

**Contributors:** Main: Prokopios Drogkaris [KEMEA]

Others: Georgios Kioumourtzis [KEMEA]  
Vasileios Kassouras [KEMEA]  
George Leventakis [KEMEA]  
Mauro Borioni [SRM]  
Juan Arraiza [VICOM]  
Liza Charalambous [ADITESS]

Emma Teodoro [EAB Member]  
Lilian Mitrou [EAB Member]  
Alfonso Alfonsi [EAB Member]

Every effort has been made to ensure that all statements and information contained herein are accurate; however the Partners accept no liability for any error or omission in the same.

© Copyright in this document remains vested in the Project Partners

## Document Control

Version	Date	Author	Modifications
0.1	28/11/2014	Prokopios Drogkaris (KEMEA)	First draft
0,2	10/12/2014	Liza Charalambous (ADITESS)	Comments and Input on Section 5
1.0	29/12/2014	Emma Teodoro [EAB Member] Lilian Mitrou [EAB Member] Alfonso Alfonsi [EAB Member]	Sections 1-5 Comments
1.1	5/1/2015	Georgios Kioumourtzis [KEMEA]	Sections 1-5 Revision
1.2	12/1/2015	Mauro Borioni [SRM]	Sections 1-5 Input
2.0	26/1/2015	Emma Teodoro [EAB Member] Lilian Mitrou [EAB Member] Alfonso Alfonsi [EAB Member]	Document Review
2.1	30/1/2015	Vasileios Kassouras [KEMEA] Juan Arraiza [VICOM]	Document Review

## Table of contents

<b>1.</b>	<b>OVERVIEW .....</b>	<b>6</b>
<b>2.</b>	<b>P-REACT PLATFORM OVERVIEW .....</b>	<b>8</b>
<b>3.</b>	<b>OUTLINE OF SECURITY REQUIREMENTS .....</b>	<b>9</b>
3.1.	ACCESS CONTROL (AUTHORIZATION) .....	9
3.2.	AUTHENTICATION .....	9
3.3.	NON-REPUDIATION.....	9
3.4.	DATA CONFIDENTIALITY .....	9
3.5.	COMMUNICATION SECURITY .....	10
3.6.	DATA INTEGRITY.....	10
3.7.	AVAILABILITY .....	10
<b>4.</b>	<b>GUIDELINES .....</b>	<b>11</b>
4.1.	GUIDING DESIGN AND IMPLEMENTATION PRINCIPLES .....	11
4.2.	IMPLEMENTATION AND DEPLOYMENT GUIDELINES .....	12
4.3.	IMPLEMENTATION AND DEPLOYMENT CHECKLIST .....	14
<b>5.</b>	<b>ACTIONS UNDERTAKEN FOR THE PROTECTION OF PRIVACY.....</b>	<b>15</b>
5.1.	PROTECTION OF PRIVACY FOR INFORMED VOLUNTARY PARTICIPANTS .....	16
5.2.	LETTER OF REQUEST TO PARTICIPATE IN P-REACT [WORKSHOP/TRIAL].....	17
5.3.	P-REACT INFORMATION SHEET .....	18
5.4.	P-REACT INFORMED CONSENT FORM .....	19
<b>6.</b>	<b>ETHICAL ADVISORY BOARD RECOMMENDATIONS .....</b>	<b>20</b>
<b>7.</b>	<b>CONCLUSIONS .....</b>	<b>22</b>

## Annexes

<b>ANNEX I. GLOSSARY AND ACRONYMS .....</b>	<b>23</b>
<b>ANNEX II. REFERENCES .....</b>	<b>24</b>



**Project**

Petty cRiminality diminution through sEarch and Analysis in multi-source video Capturing and archiving plaTform

**Phase**

WP1 – Project Management

## Tables

TABLE 1: GUIDING DESIGN AND IMPLEMENTATION PRINCIPLES .....	12
TABLE 2: IMPLEMENTATION AND DEPLOYMENT GUIDELINES.....	14
TABLE 3: IMPLEMENTATION AND DEPLOYMENT CHECKLIST .....	14
TABLE 4: EAB RECOMMENDATIONS .....	21
TABLE 5: GLOSSARY AND ACRONYMS.....	23

## Figures

FIGURE 1: P-REACT HIGH LEVEL ARCHITECTURE .....	8
---	---

## 1. Overview

The deployment of a platform that will detect Petty Crime incidents through the installation of low-cost components in the premises of small business or transportation operators, which will be networked with one or more cloud based services raises several concerns related to privacy and ethical issues. Even if the objective of P-REACT project is to develop, demonstrate and validate a solution capable of fighting criminality and at the same time meet the needs and financial expectations of the communities, citizens and businesses, it is apparent that prior to the (commercial) exploitation of the platform, key privacy and ethical concerns identified along to its use by the potential end users must be addressed and clearly defined by each potential proprietor/owner.

P-REACT's DoW describes deliverable D1.6 - Guidelines for Ethical, Privacy and Data Protections Issues: *A set of principles taking into account the key ethical and privacy concerns. Detailed information will be provided regarding privacy and confidentiality, and the procedures that will be implemented for collection, storage, protection, retention, and destruction of data.* This document includes input from Task 1.3: Ethics and Societal Issues Management, including D 1.5 – Privacy Impact Assessment, where, a set of questions have been putted together towards uncovering privacy risks and the severity level of the potential risks of ethical and legal breaches that P- P-REACT system poses was defined through the Traffic Light system. The outcome of the assessment was positive, since the requirements and limitations related to fundamental principles of data protection legislation, lawfulness of data processing and retention, data subject's privacy rights and technical security aspects are fulfilled to an acceptable level. During the early stages of the P-REACT project, the consortium has thoroughly considered the ethical guidelines set out by the Seventh Framework Programme in addition to all respective EU legislation, international conventions and declarations pertaining:

- the Charter of Fundamental Rights of the European Union,
- the European Convention for the Protection of Human Rights and Fundamental Freedoms,
- 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 and
- EU Data Protection Regulation Reform Proposal

The objective of this document is to provide guidelines that will provide simple and practical help during the implementation and validation stages of the platform, support compliance on underlying legal framework and promote the adoption of best privacy practices including Privacy Enhancing Technologies.

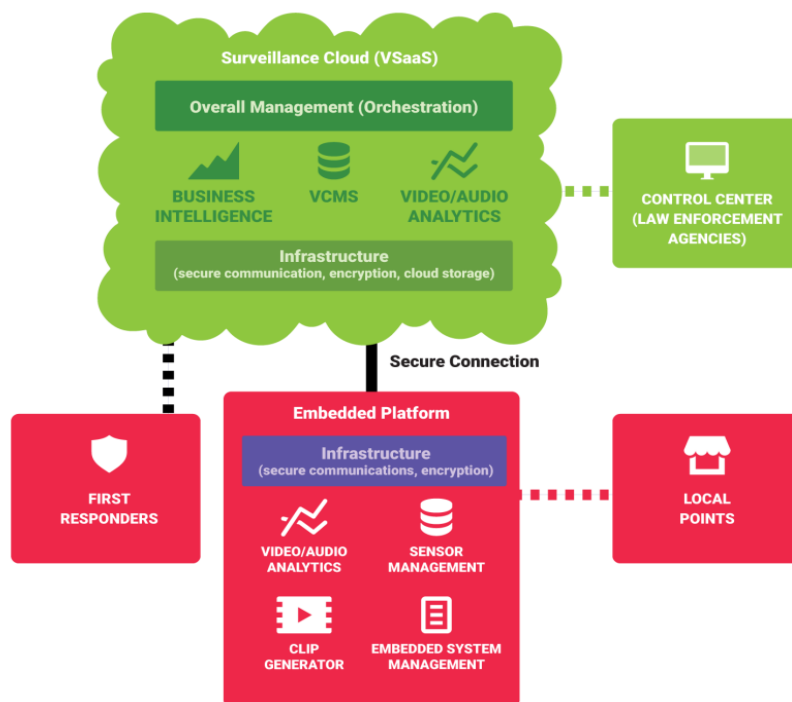
This document includes the following sections:

- **Section 2** - provides an overall high level description of the P-REACT platform
- **Section 3** - provides an outline of the identified security requirements that have stemmed from privacy related concerns
- **Section 4** - presents the Ethical, Privacy and Data Protection guidelines proposed that stemmed from the fundamental principles that we adopted by the project
- **Section 5** - presents the preparatory actions undertaken towards the protection of Privacy of participants
- **Section 6** - presents the recommendations of the Ethical Advisory Board external members and finally
- **Section 7** - concludes this deliverable.

## 2. P-REACT Platform Overview

An overall high level architecture of P-REACT platform is presented and briefly discussed in this section. A deeper analysis of the P-REACT platform architecture and its modules is documented in *D2.3 P-REACT Conceptual Architecture*, including functional, technical and large-scale deployment specifications. The architecture design has two main components: (i) local embedded platform and (ii) cloud service and is presented in Figure 1 below. Moreover the architecture includes the end-user interface.

P-REACT architecture has been designed in a modular way in order to support in the future more powerful embedded systems and algorithms mainly for video and audio analytics. In addition to this, the architecture allows using the appropriate video and audio analytics algorithm(s) for a specific case which can be downloaded from the cloud to the embedded system improving the flexibility and scalability of the proposed platform. Either the new video or audio analytic algorithm can be automatically pushed to a neighbour embedded system when an event trigger send to the Video Software as a Service (VSaaS) cloud or when trigger send to the VSaaS cloud and needs further examination at the local point.



**Figure 1: P-REACT High Level Architecture**



## 3. Outline of Security Requirements

For P-REACT system to respect ISO/IEC 27001 standard the following security requirements have been identified and are presented in D2.2 - P-REACT Local Embedded framework and system on the cloud requirements and D2.3 - P-REACT Conceptual Architecture are briefly presented below.

### 3.1. Access Control (Authorization)

P.REACT system must be capable of controlling the level of access that each pre-defined level/ (category) of user(s) has depending on their role and the required levels of protection for each component. There must be appropriate mechanisms to define and enforce such access control (e.g. firewalls, file systems permissions, secure log-in) including physical control of access to both embedded platform and cloud system terminals.

### 3.2. Authentication

Authentication mechanisms deployed must guarantee that the system being accessed is the intended one and that the user is who claims to be.

### 3.3. Non-Repudiation

In order to ensure the admissibility of digital data managed as evidentiary material to the incident, the capability to prevent users from denying that data files were accessed, altered or deleted, highly-secure logging and auditing processes must be implemented.

### 3.4. Data Confidentiality

The protection of information from unauthorized access and disclosure must be preserved by defining and/ or restricting per-user-group access to every type of information dealt with and encrypting the information during transmission and also during storage. Within the scope of the project, the use of a cloud infrastructure may result to additional risks and the deployment should be based on a private cloud infrastructure, deployed and used solely for the purposes of the project. The same level of protection should also be applied, after the defined retention period expires, during the information erasure/destruction. More specifically for information destruction the undertaken methodologies could include Re-formatting, overwriting or degaussing.

### **3.5. Communication Security**

To ensure that communication only flows from a source to the intended destination, all communication between the Embedded System (ES) and the Cloud must be made through encrypted communication channels.

### **3.6. Data Integrity**

P-REACT system should protect data from unauthorized, uncontrolled, or accidental alteration during storage or transmission with the use of checksum values, hash functions and digital signatures.

### **3.7. Availability**

Back-up mechanisms are a desirable property, mainly to avoid Denial of Service (DoS) attacks however the exploitation of a cloud infrastructure could provide an adequate assurance for the scopes of the project.

## 4. Guidelines

In order to ensure that the developed system addresses the concerns of individuals on fundamental privacy and ethical issues, a set of guiding principles has been adopted at the early stages of the project, based on the Surveillance Camera Code of Practice Document that has been published by the UK Home Office in 2013 [1] and following the requirements and considerations identified in D. 2.2 - P-REACT Local Embedded framework and system on the cloud requirements. Based on these principles and following the findings of PIA and the EAB Initial Recommendations included within D.1.5 – Privacy Impact Assessment, which was focused on ensuring that ethics awareness and surveillance are fully integrated into the project. Finally, in order to monitor the implementation and compliance with the aforementioned guidelines, a Checklist has also been created as an additional measure to monitor and evaluate the implementation and validation procedures.

### 4.1. Guiding Design and Implementation Principles

Guiding Principles	
<b>G.P. 1</b>	Use of the P-REACT system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
<b>G.P. 2</b>	The use of P-REACT must take into account its effect/impact on individuals and their privacy, with regular reviews to ensure its use remains justified.
<b>G.P. 3</b>	There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints
<b>G.P. 4</b>	There must be clear responsibility and accountability for all surveillance camera system activities including images and information collection, storage and use.
<b>G.P. 5</b>	Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who has to comply with them.
<b>G.P. 6</b>	No images and information should be stored beyond which is strictly required for the stated purpose of the specific surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

<b>G.P. 7</b>	Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
<b>G.P. 8</b>	Surveillance camera system operators should consider any approved operational, technical and security standards relevant to a system and its purpose and work to meet and maintain those standards.
<b>G.P. 9</b>	Images and information collected and stored through surveillance camera system should be subject to appropriate organisational and technical security measures against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
<b>G.P. 10</b>	There should be appropriate and effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular audit reports should be published.
<b>G.P. 11</b>	Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

*Table 1: Guiding Design and Implementation Principles*

## 4.2. Implementation and Deployment Guidelines

	<b>Guidelines</b>
<b>GL. 1</b>	The purpose of the deployed platform must be established and clearly defined prior to its deployment (security of persons and goods, deterrence, prevention, evidentiary material to the incident)
<b>GL. 2</b>	The expected outcomes of the system, the type of technologies, equipment and infrastructure that will be used must be defined and clearly described
<b>GL. 3</b>	A Data Protection Officer must be assigned for both the embedded platforms and the cloud

	system
<b>GL. 4</b>	The deployment of the equipment must be performed in a way that will not intrude disproportionately / to a disproportional extent on the privacy of individuals (image and audio quality, zoom and rotation, Intrusive camera locations)
<b>GL. 5</b>	The scope of legitimate purpose/use and limitations on the use of the data must be clearly established in order to avoid further incompatible use.
<b>GL. 6</b>	Information to the public must be provided in an effective and comprehensive manner following a multilayer approach. It will combine methods such as on-the-spot notice boards and a detailed data protection notice posted on the Institution’s intranet and internet sites.
<b>GL. 7</b>	Technical descriptors of the lists of events (based on behaviors and not physical characteristics such as gender, age or ethnic group identification) associated with each petty crime must be provided in order to identify possible adverse effects in terms of stigmatization or discrimination of individuals. The level of accuracy of the event detection should be carefully considered
<b>GL. 8</b>	The form and the content of the alerts must be clearly defined and they must be based on incidents not on targeted individuals
<b>GL. 9</b>	Clip Database must be administered by a designated administrator
<b>GL. 10</b>	Adequate technical and procedural measures must be in place on ensure that all collected, stored and processed are protected from loss, unauthorised access, use, modification and disclosure.
<b>GL. 11</b>	The retention period of all data and information collected, stored and processed must not me longer that it is necessary to achieve the purpose collected and the period specified within the applicable National Laws and EU Directives.
<b>GL. 12</b>	Generalized searches from authorized users based on “sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation must be prohibited
<b>GL. 13</b>	The request concept , ie access requests to data clips and data stored needs to be defined and provide clear distinction between different types of requests (normal request, official

	request, and judicial request) in order to provide data from the system to the potential end users.
<b>GL. 14</b>	Different types of users and their access, modification, request and deletion rights must be explicitly specified.
<b>GL. 15</b>	Each user must be uniquely identified when accessing the platform through mechanisms that provide adequate level of assurance on her real-life identity.
<b>GL. 16</b>	A reliable digital logging system must be implemented to conduct an audit at any time needed.
<b>GL. 17</b>	Appropriate procedures must be defined to respond to any inadvertent disclosure of personal information
<b>GL. 18</b>	The encryption algorithm deployed must be defined.
<b>GL. 19</b>	Appropriate procedures must be defined to comply with data subjects' requests to exercise their rights.

*Table 2: Implementation and Deployment Guidelines*

### 4.3. Implementation and Deployment Checklist

		Date:		
		Checked		Comments
Guidelines	GL. 1	Yes	No	
	GL. 2			
	GL. 3			
	GL. 4			
	...			
	GL. 19			

*Table 3: Implementation and Deployment Checklist*

## 5. Actions Undertaken for the Protection of Privacy

The P-REACT consortium places high value on the need to protect citizens' data and privacy and all respective EU regulations and main Data Protection Principles, and therefore has been made sure that the following principles will be respected throughout the lifecycle of the project:

- Proportionality principle / Data minimization – Only adequate, relevant and no more data than strict necessary.
- Purpose limitation principle – specified/pre-defined/ explicit/ legitimate initial purpose – Prohibition of secondary use / for purposes not compatible with the initial purpose
- Assessment. By assessing the proportionality between (private/public) interests to be protected means to be used and invasion/harm for the participating individuals
- Accuracy /Up to date - Clear distinctions between 1) personal data of i) survey participants, ii) pilot participants, iii) third parties and 2) degrees of accuracy and reliability of personal data (evidence, assessment etc.)
- Time-limited identified/identifiable information kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed.
- Security of storage and access rights by designing –implementing appropriate measures and processes.

Specifically, regarding pilot demonstrations and other relevant foreseen activities that may require involvement of informed voluntary participants', consent forms and information sheets will be provided to all individuals. In order to ensure respect for human dignity, fair distribution of research benefits and burden and protecting the values, rights and interests of the voluntary research participants all personal data collected will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary

- Processed in accordance with the data subject's rights
- Secure
- Not transferred to countries without adequate protection
- 

Prior to the commencement of P-REACT research activities, all respective Data Protection Agencies (DPA) of the countries of the partners belonging to the P-REACT project have been notified (Greece, Italy, Cyprus, Spain, Ireland, UK). The introductory letter and the respective notification documents have been submitted with D.1.4 - Quality Policy. In addition to these notifications, before pilot testing phases of the P-REACT, the respective National Data Protection of the participant's countries that the pilots will take place will be notified of the projects pilot phases and more specifically on the personal data of the voluntary participants that will be utilized by the developed Data Sets. Additional information on notification procedures and the relevant agencies in Europe will be sourced from the Article 29 Working Group document "Vadmeccum on Notification Requirements"

## **5.1. Protection of Privacy for Informed Voluntary Participants**

All informed voluntary participants, who agree to participate at the pilots, will be provided with an information sheet describing their privacy rights along with a brief description of the project activities, which information are to be collected and how this information will be used, processed and stored along to the respective retention periods.

More specifically, they will receive in their own language:

- a commonly understandable written description of the project and its goals;
- the planned project progress and the related testing and evaluation procedures;
- advice on unrestricted disclaimer rights on their agreement.

Additionally, all voluntary participants will receive, in their own language, a Letter of Consent which they will be asked to sign and return back. Within this letter there will be included:

- a description of their rights according to the respective data protection law
- a description of the information that will be collected
- a description of how this information will be used, processed and stored along to the respective retention periods
- a description of alongside activities (such as dissemination activities) that will make use of



this information.

- a statement of basic principles on which the collection, storage and processing will be based on.

A provisional version of the invitation letters to be sent to voluntary participants, Information Sheet and Informed Consent Form is presented in the following sections. The final versions will also be approved by the EAB.

## 5.2. Letter of Request to participate in P-REACT [Workshop/Trial]



Dear [Name],

I am writing to you on behalf of P-REACT project ([Petty cRiminality diminution through sEarch and Analysis in multi-source video Capturing and archiving plaTform](#)), a 24-month EU-funded project. Its objective is to design and develop a low cost surveillance platform that will ensure communication between key users with a focus on increasing the ability of Law Enforcement and security personnel to respond to minor crime events such as theft, trespassing etc. The solution will encompass intelligent video and audio sensors to detect volume crime incidents, a cloud based monitoring, alert detection and storage platform.

As part of P-REACT project, a [workshop/ trial] is to be convened, to identify, elicitate, discuss and validate initial user requirements as well as collecting feedback about the prototypes of the P-REACT platform.

I am seeking your participation in one of the [workshop/ pilot] that will take place at [date, location]

The P-REACT consortium assures you that any personal data or information you provide will be kept strictly confidential and will be securely stored and retained for the lifetime of the project, deleted thereafter and used solely for the purposes of the project without any secondary use during this period. Furthermore, should you agree to participate, and subsequently feel unable or unwilling to continue, you are free to leave without any further consequences. That is, your participation is completely voluntary,

and you may withdraw from this project at any time. Following your request to withdraw, all your personal data collected and stored by will also be deleted.

During this [workshop/pilot], [organizing partner] will take all appropriate measures to make the area, not accessible to general public, before the commencement and during these activities. Trials will take place during off-hours, all designated areas will be marked and perimeter security measures will be deployed, including access control, so that only accredited individuals with specific roles and responsibilities will be able to access them

An information sheet, which describes the project in greater detail, has been prepared (see attached) to help you make a fully informed decision on participation. Should you agree to participate, after understanding and accepting the conditions, we will provide you with a consent form on the day of the [workshop/ interview/pilot demonstration] that will formalize the conditions of your participation.

Should you require any additional information, please do not hesitate to contact me directly.

Looking forward to your response.

Best Regards,

[Project Coordinator / Pilot Partner Contact Details]

### 5.3. P-REACT Information Sheet



- P-REACT project involves human research subjects
- The purpose of this research is to design and develop a low cost surveillance platform that will ensure communication between key users with a focus on increasing the ability of Law Enforcement and security personnel to respond to minor crime events such as theft, trespassing etc. The solution will encompass intelligent video and audio sensors to detect

volume crime incidents, a cloud based monitoring, alert detection and storage platform

- Participation to this research is on a voluntary basis
- The research is funded by the European Union’s Seventh Framework programme under Grant Agreement 607881
- The following benefits to the subject or to others which may reasonably be expected from the research avoiding inappropriate expectations.
- Should you have any further questions, or wish to withdraw at any time from the research without consequences, please contact:
- [Project Coordinator / Pilot Partner Contact Details]
- All data related to this research will be available only to the consortium partners and the European Commission, will be used only within the scope of the project and will be securely erased afterwards.

## 5.4. P-REACT Informed Consent Form



*Please answer the following questions by ticking the response that applies*

	<b>YES</b>	<b>NO</b>
1. I have read the Information Sheet for this study and have had details of the study explained to me.	<input type="checkbox"/>	<input type="checkbox"/>
2. My questions about the study have been answered to my satisfaction and I understand that I may ask further questions at any point.	<input type="checkbox"/>	<input type="checkbox"/>
3. I understand that I am free to withdraw from the study within the time limits outlined in the Information Sheet, without giving a reason for my withdrawal or to decline to answer any particular questions in the study without any consequences to my future treatment by the researcher.	<input type="checkbox"/>	<input type="checkbox"/>
4. I agree to provide information to the researchers under the conditions of	<input type="checkbox"/>	<input type="checkbox"/>

confidentiality set out in the Information Sheet.

5. I wish to participate in the study under the conditions set out in the Information Sheet.
6. I consent to the information collected for the purposes of this research study, once anonymised (so that I cannot be identified), to be used for any other research purposes within the scope of P-REACT project.

**Participant’s Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

## 6. Ethical Advisory Board Recommendations

The EAB has closely monitored the process of definition of the Guidelines for Ethical, Privacy and Data Protection Issues, providing feedback to the different versions of D1.6. This process focused on the analysis of the way in which the guidelines responded to: 1) the risks identified in the Privacy Impact Assessment (PIA) performed previously and included in D1.5. and 2) to the Initial Recommendation provided by the EAB in the former document.

This analysis is presented in the following Table. The table presents the link between each one of the Initial Recommendations of the EAB and the corresponding Guidelines, both in the phase of Design and Implementation (4.1) and in the second phase of Implementation and Deployment (4.2).

The EAB acknowledges the fact that all the Initial Recommendations have been translated to the guidelines presented in Section 4 of this deliverable. Nevertheless, some remarks have been included in those cases when the EAB has considered that some issues arise from the way in which that translation has been made from recommendation to guideline.

This process- in which the EAB checks the implementation of its own previous recommendations- allows for an accurate review of the ethical and privacy related issues that arise during the development of the project. The EAB is therefore, performing what could be called interim ethical audits of the project, thus making sure that as it evolves, the P-React platform complies with the applicable legal requirements and ethical values. In this way the EAB is defining the framework for the Mid-term recommendations to be included in D.1.2

EAB Initial Recommendations	4.1 G.P.	4.2 G.L.	EAB Remarks
R.1	1, 11,6	1, 5	The guidelines should refer to the specific purpose of the P-React Project and not in general to the existence of a given purpose. The concept of “pressing need” should be further defined.
R.2	5, 3	6, 19	
R.3. /R.4			Reference to recommendations 3 and 4 are included in section 5 of the deliverable. However direct reference should be made to the information sheet and the informed consent letter as one of the Guiding design principles.
R.5		7	
R.6		8	
R.7		12	The issue of specific searches based on such features should also be addressed, defining whether those searches are allowed and under which conditions.
R.8		13	The implementation guidelines should provide the definition of the concept of request to be used by the P-React system.
R.9	4, 9, 10	10,14,15, 16	
R.10		10, 17	
R.11		13	
R.12		9	There is a need to further define the potentially risky elements identified in the PIA and included by the EAB in R.12.

*Table 4: EAB Recommendations*

## 7. Conclusions

Following the risks identified in the Privacy Impact Assessment (PIA) and the Initial Recommendation provided by the EAB, this document has provided guidelines that will deliver simple and practical help during the implementation and validation stages of the P-REACT platform, support compliance on underlying legal framework and promote the adoption of best privacy practices including Privacy Enhancing Technologies. Subsequent to a high level presentation of the architecture and an outline of the identified security requirements that have stemmed from privacy related concerns presented in Sections 2 and 3, Section 4 presented the Ethical, Privacy and Data Protection guidelines that stemmed from the fundamental principles that were adopted at the early stages of the project. These guidelines cover aspects such as data processing, storage, retention and destructure, legal compliance and compliance with market standards and best practices, privacy and informed consent in addition to improper use. Taking an additional step, an one-to-one checklist is also presented as the monitoring tool of evaluating the implementation and validation procedure results. At the time this report was written, the data sets to be utilized by the platform have not been fully defined and therefore their description and the exact procedures to be adopted have not been discussed extensively. Upon their definition, an attempt to identify newly introduced risks, compliance with the adopted guidelines and discussion on the procedures implemented will be performed. Finally, Section 5 presented the actions undertaken so far towards the protection of Privacy of informed participants through the notification of all respective National Data Protection Authorities and the provisional documents to be delivered to all volunteer participants, prior to their involvement in the project activities and Section 6 includes the recommendations of the Ethical Advisory Board external members.

## ANNEX I. GLOSSARY AND ACRONYMS

Term	Definition / Description
CCTV	Closed-Circuit television
EAB	Ethical Advisory Board
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
PIA	Privacy Impact Assessment
VCMS	Video Content Management Server
VPN	Virtual Private Network
VSaaS	Video Software as a Service

*Table 5: Glossary and Acronyms*

## ANNEX II. REFERENCES

The table below shows the most significant references used and/or cited to prepare this document:

Reference	Source
-----------	--------

### Works Cited

- 1 UK Home Office: Surveillance Camera Code of Practice.  
. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/204775/Surveillance\\_Camera\\_Code\\_of\\_Practice\\_WEB.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf) (2013)
- 2 Article 29 Data Protection Working Party: Working Document on the Processing of Personal Data by means of Video Surveillance., [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67_en.pdf) (2002)
- 3 European Commission: Communication from the Commission to the Council and the European Parliament - Crime prevention in the European Union /\* COM/2004/0165 final \*/., <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52004DC0165&from=EN> (2004)