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

Deliverable D2.1
Report on the Data Protection, Privacy, Ethical and Criminal Law Frameworks
Work Package 2 - Data Protection Privacy, Ethical and Criminal Law (DaPPECL) Restraints

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.

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

<table>
<thead>
<tr>
<th><strong>Project short name and number</strong></th>
<th>FORENSOR (653355)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Work package</strong></td>
<td>WP2</td>
</tr>
<tr>
<td><strong>Number</strong></td>
<td>D2.1</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>Report on the Data Protection, Privacy, Ethical and Criminal Law Frameworks</td>
</tr>
<tr>
<td><strong>Responsible beneficiary</strong></td>
<td>VUB</td>
</tr>
<tr>
<td><strong>Involved beneficiaries</strong></td>
<td>VUB, ALMA, VIS</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>R</td>
</tr>
<tr>
<td><strong>Dissemination level</strong></td>
<td>PU</td>
</tr>
<tr>
<td><strong>Contractual date of delivery</strong></td>
<td>29.02.2016</td>
</tr>
<tr>
<td><strong>Last update</strong></td>
<td>v 1.00 29.02.2016</td>
</tr>
</tbody>
</table>

---

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Status</th>
<th>Authors, Reviewers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v 0.01</td>
<td>01.10.2015</td>
<td>Template</td>
<td>CERTH</td>
<td>Project deliverable template.</td>
</tr>
<tr>
<td>v 0.02</td>
<td>01.11.2015</td>
<td>Draft</td>
<td>Paul Quinn</td>
<td>Table of contents and document structure.</td>
</tr>
<tr>
<td>v 0.03</td>
<td>15.01.2016</td>
<td>Draft</td>
<td>Paul Quinn, Dariusz Klosa</td>
<td>Draft 1</td>
</tr>
<tr>
<td>v 0.24</td>
<td>08.02.16</td>
<td>Draft</td>
<td>Paul Quinn, Dariusz Klosa, Paul De Hert</td>
<td>Final draft before review</td>
</tr>
<tr>
<td>v 0.25</td>
<td>20.02.2016</td>
<td>Draft</td>
<td>Dessy, Yankova of JCP, Filipe Custódio of VIS</td>
<td>Minor comments received from Desislava Yankova of JCP Connect. Some legisilative material concerning Portugal added,</td>
</tr>
<tr>
<td>v 0.26</td>
<td>26.02.2016</td>
<td>Final Draft</td>
<td>Paul Quinn, Dariusz Klosa, Paul De Hert</td>
<td>Final draft before submission</td>
</tr>
<tr>
<td>v 1.00</td>
<td>29.02.2016</td>
<td>Final</td>
<td>Lazaros Gymnopoulos</td>
<td>Final document for submission.</td>
</tr>
</tbody>
</table>
Contents

1 Executive Summary ......................................................................................................................... 7
   1.1 Privacy concerns and FORENSOR ......................................................................................... 7
   1.2 The importance of general privacy laws to the FORENSOR project ......................... 8
   1.3 The importance of data protection laws .............................................................................. 8
   1.4 FORENSOR and rules of evidence .................................................................................... 9

2 Introduction .................................................................................................................................... 12

3 The Concepts of Privacy, Surveillance and Security ............................................................................ 14
   3.1 Privacy as a Concept ............................................................................................................. 15
      3.1.1 Autonomy as a potential linking concept ................................................................. 16
      3.1.2 Informational privacy as a prominent form of privacy ........................................... 17
      3.1.3 Privacy and Surveillance – The need for a wide conception of privacy .......... 18
      3.1.4 Data Protection as an Approach to Promote Individual Privacy .................... 20
   3.2 The need to foster security as a counterweight to privacy ............................................... 20
      3.2.1 A right to privacy can not be absolute ............................................................... 20
      3.2.2 Infringements upon privacy should be of a proportional nature .................. 21
   3.3 Relevance of the privacy v security paradigm for the FORENSOR project .......... 23

4 Privacy (in the broad sense) in law ................................................................................................. 24
   4.1 Prominent protection for privacy found in international treaties .................................. 24
   4.2 Privacy at the European Level ............................................................................................. 25
   4.3 The ECHR and privacy the context of surveillance technologies and practices .......... 26
      4.3.1 The contribution of privacy by design and privacy enhancing technology to the question of proportionality ................................................................. 29
      4.3.2 General privacy approaches – key points for the FORENSOR project .......... 29

5 Data Protection – A Prominent Legal Approach Concerned with Privacy in the Informational Sense .......................................................................................................................... 30
   5.1 FORENSOR and personal data ......................................................................................... 31
   5.2 The Council of Europe’s data protection approach ....................................................... 32
   5.3 The EU’s Data Protection Approach ............................................................................... 32
      5.3.1 Fundamental Commitments in Primary Law ............................................................. 32
      5.3.2 EU Legislative Initiatives (Secondary Law) ............................................................... 33
      5.3.3 The main regulatory actors concerned with privacy and data protection .......... 34
      5.3.4 Data Protection Requirements of Potential Application to the FORENSOR project 34
   5.4 Transferring data across borders ....................................................................................... 39
      5.4.1 Within the EU ........................................................................................................... 39
      5.4.2 Outside the EU ......................................................................................................... 40
   5.5 Examples of data protection law in various member states of the EU ....................... 41
   5.6 The proposed EU Data protection regulation ................................................................... 42

6 Rules and Principles pertaining to the Use of Images and Videos in Criminal Proceedings ................................................................................................................................. 44
   6.1 General Rules Concerning Due Process in Criminal Proceedings ............................. 45
6.1.1 Fairness ........................................................................................................ 46
6.1.2 Quality .......................................................................................................... 47
6.1.3 Issues related to entrapment ........................................................................ 47
6.1.4 Appropriate oversight ................................................................................ 48
6.2 Common rules and principles pertaining to digital evidence ....................... 48
6.3 General Precautionary Principles to be applied to digital evidence ............. 50

7 Annex I – Examples of The Imposition of Data Protection Law in Use Case
Member States ...................................................................................................... 56
7.1 Portugal ............................................................................................................ 56
  7.1.1 Background .................................................................................................. 56
  7.1.2 Salient Examples ......................................................................................... 57
7.2 Greece ............................................................................................................. 62
  7.2.1 Background .................................................................................................. 62
  7.2.2 Salient National Law .................................................................................. 62
7.3 Italy ................................................................................................................. 70
  7.3.1 Background .................................................................................................. 70
  7.3.2 Salient Examples of National Law ................................................................. 71
7.4 Spain ............................................................................................................... 75
  7.4.1 Background .................................................................................................. 75
  7.4.2 Salient Examples of National Law ................................................................. 77

8 Annex II – Relevant Provisions of the Council of Europe’s Convention on
Cybercrime ........................................................................................................... 84

9 Annex III – An Abstract of the Local Data Protection Laws in Chiusi Village ...... 87

10 Annex IV - Principles in Portuguese Law Relating to Criminal Evidence and the
Concept of Proportionality ...................................................................................... 92
1 Executive Summary

The information presented below outlines the main findings of this deliverable.

1.1 Privacy concerns and FORENSOR

The often competing nature of claims related to privacy and security are obviously relevant in the context of the FORENSOR project. FORENSOR by its very nature is something that poses a risk to privacy. Whether this be in the narrow informational sense or the broader sense (i.e. privacy as freedom from unnecessary steering) this is something that is important to consider. With regards to the former, it is important to discern if, where and how FORENSOR will make use of information pertaining to identifiable individuals. Where it does it will be necessary to comply with frameworks that are established in order to protect personal data. With regards to the latter it is important to recognize that privacy need not only relate to information concerning specific individuals but can also be thought of in a wider sense. Surveillance activities that are not likely to use individual information may still exert psychological pressure upon individuals that may be capable of altering their behavior. Individuals may not feel comfortable acting in a way that they may have otherwise have done so if they feel they are being monitored or if they feel that their simple presence may draw unwanted attention. Such aversion may even be the case where people are not committing illegal activities but for one reasons or another may not want people to be aware of their presence in a certain place at a certain time.

Such potential infringements on personal privacy (whether it be in the narrow informational or broader sense) are not always unacceptable however. This includes potential uses in incidences relating to crime and security for which FORENSOR is intended. Depending on the level of infringement of privacy that occurs and the intended use, the deployment of FORENSOR devices may be acceptable in certain occasions. The concept of proportionality provides a useful way of judging when such infringements may be acceptable. In terms of possible infringements upon privacy, imagine for example the difference between cameras viewing private property or public areas. Imagine also the difference between a surveillance system that is activated by all passers by and a surveillance system that is only activated by certain events that are more likely to correlate to criminal activity. Imagine also the aim of the measures in question. Are they intended to tackle serious crime (e.g. drugs smuggling or other organized crime) or are they intended to tackle petty criminality (e.g. dropping of litter or illegal parking). In deciding upon whether a potential use would be acceptable it would be necessary (and proportional) to take all such factors into account.
1.2 The importance of general privacy laws to the FORENSOR project

The proposed FORENSOR prototype represents a technology that will be used for surveillance purposes. As such, the FORENSOR device, when used for such purposes will be capable of infringing on the privacy of individuals. Such infringement will occur whether such surveillance occurs in busy public areas, secluded public areas or private property (though the infringement will be of a much graver nature in the latter case). Whilst such actions may be infringements of privacy, they may not, depending on the context in question be illegal. This is because in many contexts such surveillance measures may be necessary and proportional in order to address issues of crime and public order. Article 8 ECHR recognizes this by offering a qualification to its general protection inter alia for measures that are intended to prevent crime. This does not mean that the mere fact that where a ‘Forensor like’ device is used in order to detect or prevent crime it will automatically be legal. This is because the use of such a device in a particular context would have to meet the conditions of having being both described in law and being necessary and proportional. The FORENSOR project itself is not in a position itself to address the first of these issues – that is something that only national and regional legislators can address. Once again the particular context in question is also something that the FORENSOR project will not be able to influence – that is choice of the particular law enforcement agency ‘on the ground’ to decide upon i.e. on the particular local conditions that may require the deployment of the device. Where FORENSOR as a research project is however able to make a realistic difference to this question of proportionality, and therefore by extension the potential legality of a particular use, is by making the design of the device in question as ‘privacy friendly as possible’. This need prevents both an opportunity and an imperative to incorporate ‘Privacy by Design’ (PBD) in the design and development of the FORENSOR prototype. Through doing so (e.g. by designing the device in a way so that it only records activity at certain times or activity that is highly likely to be only of a criminal nature) the chances are higher that the use of the device in a particular circumstance will be deemed as being proportional. This is important given that it is something that will be paramount in the minds of the police, prosecutors and investigative judges when they are deciding upon requests to deploy the device. A failure to do so would run the risk that the FORENSOR device could only be used in the most grave of contexts (i.e. involving very serious criminality) and would reduce both its appeal and potential uptake.

1.3 The importance of data protection laws

The EU’s data protection approach applies when personal data is being processed. Personal data is defined in Directive 95/46/EC (Article 2) as "any information relating to an identified or identifiable". Where data can not be linked to a specific individual it will not be classed as
‘personal data’ and thus not enjoy the protection of the EU’s data protection framework. At the time of writing it is still not certain whether a FORENSOR prototype would involve the use of personal data. This is because the quality of the images captured by the device is not likely to be sufficient to identify individuals e.g. through facial images or license plate numbers on cars. Given that this is not yet certain it is wise to consider the potential impact of data protection legislation should this happen. Furthermore, the development of the FORENSOR prototype is is likely to involve trials and experimentation that may involve the use of personal data. This may for example occur where images of volunteers are recorded for modeling purposes. Research for the FORENSOR project may inter alia involve the use of conventional filming equipment for modeling purposes. It is important to consider the application of data protection legislation to both of these contexts (i.e. the use of a FORENSOR prototype for matters of criminal investigation and the use of personal data for research purposes in the FORENSOR project). In particular, FORENSOR when it uses personal information in the context of research will have to pay careful attention to issues associated with:

- The need for a correct legal basis for the processing of data
  - Most likely to be consent in the context of research within the FORENSOR project.
- The need to process data in a manner consistent with good processing principles including:
  - Data minimization
  - Data security
  - Confidentiality of data
  - The right to review and correct data
- Rules pertaining the transfer of data to third countries outside the EU

1.4 FORENSOR and rules of evidence

The aim of the FORENSOR project is to develop a prototype that will not only be capable of alerting the police and other authorities to the possible existence of criminal activities and other issues, but also to provide material that could be used as evidence in criminal proceedings. In order to be able to made use of in such a manner the data that is used will have to have been collected, stored, and handled in a manner that is not only consistent with laws concerning human rights issues surveillance and data protection issues, but also with rules concerning the gathering and use of evidence in criminal proceedings.
Failure to consider such rules will mean that images and videos gathered from the FORENSOR device will not be capable of being used in criminal proceedings. Three types of rules would govern admissibility of digital evidence in criminal proceedings, these are:

(i) general rules concerning due process in criminal proceedings;
(ii) general rules of evidence in criminal proceedings and;
(iii) specific rules relating to digital evidence in criminal proceedings.

It will be necessary for those involved in the design of a FORENSOR prototype to be aware of these principles so that such a prototype is, to as great an extent as possible, capable of facilitating good practice with regards to the gathering and use of evidence.

Rules concerning the admissibility of evidence are primarily a matter for national legal systems. It is not possible therefore to present a single legal approach for the FORENSOR project to meet that would be acceptable in all jurisdictions. Some key elements can however be gathered from European Sources, such as the ECtHR’s interpretation of Article 6 ECHR on such issues. These include the need to address issues such as:

- Fairness;
- Quality;
- Issues related to entrapment, and;
- Appropriate oversight.

In addition, despite the fact that laws pertaining to such issues are to be found within the domain of national law, it is possible to make a number of generalization regarding the use of evidence (including digital evidence) that are likely to be of relevance for the FORENSOR project. This include;

- There is the lack of established protocol for deciding whether to admit digital evidence; however, a few general rules can be drawn. As there seems to be no “clear and precise rules governing the possibility of using [...] technology in criminal proceedings.”

---

“Due process considerations forbid the usage of illegally obtained evidence before and during the trial proceedings”; “courts exclude evidence that has been obtained as a result of the exploitation of other illegally obtained evidence.”

In order for evidence to be admissible it must be relevant, without being prejudicial, and reliable.

Evidence must be direct, not hearsay or indirect. It must relate to a fact, not to an opinion. (It is the court that can draw its own conclusion).

“Admissibility is very much related to the possibility, or not, of excluding electronic evidence without prior motive.”

Digital evidence must be authentic. Therefore information should be given to the court as to “the manner in which they made the exact copy of the seized data, along with the applications used and steps taken to gather such information” [metadata]

Evidence must be presented to the court in visible and legible form.

“It is of paramount importance that anyone handling electronic evidence prior to their examination, treat them in such a manner that will give the best opportunity for any recovered data to be admissible in evidence in any later proceedings.”

The defendant might contest digital evidence at any given time.

---

5 https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeece_en.pdf
7 http://ssrn.com/abstract=1922472. Cf. further: “The Court held that so long as it could be shown that the computer was functioning properly and was not misused, a computer record can be admitted as evidence.”
2 Introduction

This deliverable forms the first stage of the data protection, privacy, ethical and criminal law (DaPPECL) impact assessment outlined in Work Package 2. The role of this deliverable within that context is to outline in broad terms the legal and ethical principles that will apply to the FORENSOR project. These requirements will be used in D2.2 to create the ‘FORENSOR impact framework’ which will apply the requirements outlined to the FORENSOR project. These requirements will be clarified with the other research partners in FORENSOR through a detailed questionnaire that will subsequently be used in D2.2 to produce the ‘FORENSOR impact assessment report’.

This deliverable outlines the most important and applicable requirements in the DaPPECL framework. In the following sections of this document each of the DaPPECL issues will be dealt with in subsequent sections. This will begin with section 3 which looks at ethical aspects of privacy and data protection that are likely to be applicable to FORENSOR. Given that FORENSOR aims to develop a novel surveillance technology it engages a number of privacy issues in a number of ways. In doing so it looks at privacy as a concept and in particular how it is difficult or even impossible to come up with a single definition of what exactly the concept is. Rather it is necessary to look at privacy in both a broader sense (i.e. related to the ability of individuals to choose their own path in life without undue steering) and in a narrower more informational sense (i.e. relating to the ability of individuals to control what is done with information that is related to them. Ethical ideas related to the former are concerned with the maintenance of a pluralist society - at the heart of which is the ability of individuals to choose their own course in life without being steered unnecessarily by outside forces that are capable of exerting both physical and psychological pressures. Indeed, ideas and ethical arguments of this type are also at the heart of legal approaches related to privacy in a general sense such as Article 8 of the European Court of Human Rights. Similar ideas are also behind principles related to informational privacy. This is because in order to preserve individual privacy it is also necessary that individuals retain sufficient control over the information that is used by them. Without such control privacy is threatened because individuals may fear acting in certain ways if they are not able to control what information about them is disclosed to others and how such information is used. Indeed, it is concepts such as these which underline legal approaches that relate to informational privacy such as data protection approaches.
Sections 4 and 5 will look at how the ethical concepts and principles described in section 3 are reflected in the law. Legal approaches relating to broader concepts of privacy (discussed in section 4) are important to consider given that they may still apply even where personal data is not involved. The most visible and perhaps the most important on the European scale is the approach developed by the European Court of Human Rights (ECtHR) under Article 8 of the European Convention of Human Rights. The ECtHR has *inter alia* stated that Article 8 is applicable to surveillance matters. Reflecting the concepts raised in the ethical discussions in section 3, the ECtHR has not stated that such practices are automatically illegal even if they are capable of infringing upon elements of individual privacy. Certain practices aimed at detecting crime or maintaining public order may be acceptable where they are necessary, proportional and outlined in law for example. Such requirements of necessity and proportionality are important elements for the designers of a potential FORENSOR prototype to consider. In particular, it will be important to consider the use of ‘Privacy by Design’ and other privacy boosting approaches given they will mean that the use of the FORENSOR device in a particular context is more likely to be seen as proportional by a court.

In terms of informational privacy it is important to take into account legal regimes concerning data protection and in particular the data protection approach of the European Union. This regime applies to the use of personal data. It is not yet certain how (or if) a FORENSOR prototype would make use of personal data given that the expected low resolution quality of the images produced may mean that individuals can not be identified (e.g. though images of faces and other identifying features such as number plates). Given that this can not be ruled out it is however important to review the data protection framework given the strict requirements it may entail if engaged. Furthermore during the FORENSOR project itself, the use of personal data is likely in the context of research activities. This may involve role play scenarios during the use case scenarios. The use of personal data may be more likely in such contexts given that conventional filming equipment (i.e. with a higher resolution may be used to capture images of individuals for modeling processes). Section 5 describes the most important principles of EU law on these issues and Annex I to this document gives some salient examples of national law on data protection from the jurisdictions in which the Use Case Scenarios will occur (i.e. Greece, Italy, Spain and Portugal).

Section 6 of this document will look at principles of law that are relevant to deciding what types of evidence may be used in criminal proceedings in courts. Such aspects of law are relevant from the perspective of the FORENSOR project given that it is intended that the FORENSOR project demonstrate not only the possibility for a surveillance system that is capable of alerting the
authorities to the possibility of criminal activity but also of collecting evidence that can be later used in criminal proceedings. In order to perform this later function, the use of such evidence would have to comply with national rules on the collection and the admissibility of evidence in criminal proceedings. Most of the rules relating to admissible evidence exist in national law, meaning that the legal position will vary from one state to another (at least in relevant law that is applicable). It is however possible to describe a number of general principles that will be relevant to the collection of evidence in all jurisdictions. This includes principles derived from the case law of Article 6 of the ECHR and ideas for best practice are likely to be of relevance in all jurisdictions.

3 The Concepts of Privacy, Surveillance and Security

Privacy, surveillance and security are concepts that are often invoked in discussions regarding strategies monitoring strategies used by law enforcement agencies, including the use of camera images or related practices. This section will introduce these three concepts from an ethical perspective. Such a perspective is important as each gives rise directly or indirectly to important legal principles that are likely inter alia to have an impact upon the development and utilization of a FORENSOR prototype. As this section will discuss, the concepts of privacy (and surveillance which can arguably be linked to privacy) and security both relate to duties upon the societies we live in (and in more pragmatic terms the state) to put in place the conditions that will allow us as individuals to live worthwhile lives according to our own desires and perceptions of what exactly constitutes the good life. Both values are therefore at the heart of modern pluralist democratic societies. Without either, liberty and freedom become impossible. Imagine for example a world where the state or some other malevolent party in society was able to know everything about private citizens and do with that information what it liked. Imagine equally a state that was devoid of law and order – what use would privacy in terms of one’s personal information be if one were too afraid to go where one wanted or do what one wished. As this section will discuss however, providing the basis for ensuring such values are realized does not amount to disparate or separate enterprises. Often a balance will need to be struck, so as to ensure that in attempting to achieve the realization of one of these goals, the other is not harmed to such an extend that is detrimental.

In discussing privacy in the context of a debate on public order and security it is therefore necessary to be aware of the need to maintain an adequate state of security in society if the possession privacy is in reality to amount to anything. Likewise in attempting to ensure that society is as secure as possible it is important to realize and maintain individual privacy given that
a life without adequate privacy, even in an environment that is secure from crime and disorder would not be tolerable either.

3.1 Privacy as a Concept

Privacy is a concept without a single accepted definition.\textsuperscript{10} Privacy is a term that is omni-present in our informational society. Individuals seek it, business and governments claim to respect it. It would be difficult to find an individual that did not value his or her privacy in one way or another. Despite this, if you were to ask the man in the street, those who are in a position of trust with regards to information, or even legal theorists you would be unlikely to receive a succinct and similar definition as to what exactly privacy is.\textsuperscript{11} Indeed what privacy means will be different to different individuals and groups in different contexts at different times.\textsuperscript{12} The former French justice Minister Robert Badinter for example went so far as to say that “respect for the secret of privacy was such that it went beyond definition”.\textsuperscript{13} Others have gone as far as to say that privacy is merely a term to relate to a number of problems “not related by a common denominator or core element. Instead, each problem has elements in common with others, yet not necessarily the same element — they share family resemblances with each other”.\textsuperscript{14}

The elusive nature of an agreed definition of privacy has created problems for ethics and legal scholars who normally strive to create common definitions that can be used to create legal rules. The contextual variations in which privacy is invoked and its intrinsic illusiveness as a concept have greatly complicated this task.\textsuperscript{15} A plethora of pseudonyms that are used interchangeably with privacy including ‘private life, ‘private sphere’, intimacy’ and ‘secrecy’ have only complicated this further. This has led some scholars to give up attempting to find a global definition and to rely on a more contextual approach where privacy is defined according to the context it is discussed within\textsuperscript{16}. For both legal and sociological purposes a global ‘catch all’ definition of privacy is therefore not available. Solove\textsuperscript{17} for example argued that the conceptions of privacy could be grouped in six categories:

\begin{itemize}
\item \textsuperscript{11} S. Gutwirth, Privacy and the Information Age (New York: 2002).
\item \textsuperscript{12} D. Wright, S. Gutwirth, M. Friedewald, E. Vildjiounate and Y. Punie, Safeguards in a World of Ambient Intelligence 2008). p14
\item \textsuperscript{13} C. Bennet, In defence of privacy: The concept and the regime', \textit{Surveillance and Society}, 8,(4) (2011) pp. 485-496
\item \textsuperscript{14} H. Nissenbaum, Privacy as Contextual Integrity', \textit{Washington Law Review}, 79,(2004) pp. 104-139
\item \textsuperscript{15} Examples of such contextual contexts are ‘home privacy’, ‘informational privacy’ and ‘relational privacy’. See S. Gutwirth, (2002) P34
\item \textsuperscript{16} Quote originally taken from D. Solove, \textit{Understanding Privacy}. (Cambridge: 2008).
\end{itemize}
“Despite what appears to be a welter of different conceptions of privacy, I argue that they can be dealt with under six general headings, which capture the recurrent ideas in the discourse. These headings include: (1) the right to be let alone – Samuel Warren and Louis Brandeis’s famous formulation for the right to privacy; (2) limited access to the self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of certain matters from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one’s personality, individuality, and dignity; and (6) intimacy – control over, or limited access to, one’s intimate relationships or aspects of life.”

By contrast, Rössler has analysed three dimensions of privacy:18

- Decisional privacy, which establishes a space for maneuver in social action that is necessary for individual autonomy,

- Informational privacy, i.e. who knows what about a person and how they know it (control over information relating to that person), 19

- Local privacy, i.e. privacy of the household, of one’s flat or room and thus privacy of personal objects; in modern societies it denotes a realm of life and a way of life that is bound up with this realm and is intrinsically indebted to the existence of private spaces, however varied the concrete form this may take.20

3.1.1 Autonomy as a potential linking concept

One common link between various conceptions of privacy is the concept of ‘autonomy’, i.e. that individuals be left as much as possible to define themselves and their choices in life.21 Autonomy can of course mean many things, depending on the context (partly explaining why it is easier to discuss privacy in a particular context than in a general abstract sense). This is inter alia reflected in the jurisprudence of the the ECtHR under Article 8 of the ECHR which is related to the ‘Protection of Private and Family Life’.22 Whilst most of the case law concerned with this article is related in some way to the protection of ‘individual autonomy’ the case law is usually developed in a more contextual basis depending upon the particular situation involved. The concept of privacy may for example be raised with regards to physical intrusions that prevent individuals

---

19 Ibid.,
20 Ibid.,P142
21 For more on the link between autonomy and privacy (and for some example of theories of privacy that are not linked to this concept) see: R. Post, (2001).
22 This is discussed further in section 4
from conducting themselves in the manner in which they might wish. On other occasions it may refer to the need to reduce or prevent pressures and influences that are exerted on individuals from outside sources and which are capable of having ‘steering’ effects on individual autonomy. This could for example refer to elements that exert psychological pressure on individuals. Such pressure may, depending on the context, be able to influence individuals in the behavior they choose to exhibit. Examples of such pressures could involve intrusion into individuals’ home or private spaces, the use of propaganda, interference with the freedom to choose one’s own form of education and attacks on ideas or beliefs that individuals may hold. Another important example of privacy as autonomy (and one which has obvious relevance for the FORENSOR project) might refer to issues of surveillance. This is because surveillance activities are not only passive activities collecting information that may relate to individuals but are also capable of influencing individuals and the behaviors they exhibit too. When individuals are aware they are being observed they may alter their behavior so as to avoid perceived negative consequences, including conveying information or impressions to others that may be perceived (rightfully or wrongfully as negative).

3.1.2 Informational privacy as a prominent form of privacy

Individual privacy is a concept based within the broader notion of privacy that refers to the ability of individuals to control how information pertaining to them is collected and used. Like most other conceptions of privacy it too is often linked to the concept of autonomy given that individuals may often alter their behavior as a function of the information about them that is known to others. This is because humans are social creatures and as a result attach importance to the perceptions of their piers and in society in general. As a result, individuals usually seek to control what information concerning them is made available to others, particularly where they feel that such

---

23 S. Gutwirth, (2002) Gutwirth for example refers to a need to reduce steering forces upon individuals which unduly pressure them to make decisions in certain ways.
24 P. Quinn and P. De Hert, Self respect—A “Rawlsian Primary Good” unprotected by the European Convention on Human Rights and its lack of a coherent approach to stigmatization?", The International Law of Discrimination and the Law, 14,(2014) pp. 19-53 Under the ECHR’s privacy approach for example it is recognized that there is a need to protect individuals from harmful forms of hate speech.
information could give rise to negative social consequences or related harm.\footnote{28} Harms to privacy in the informational sense usually thus refer to instances where information concerning individuals has been collected, used or made public contrary to the wishes of those concerned.\footnote{29} Legal and ethical approaches concerned with informational privacy are accordingly often directed and preventing misuse of information related to individuals without their consent.\footnote{30} Notions concerned with individual privacy may give rise legal approaches concerned with control over personal images, communications, information pertaining to health, patient confidentiality and many other aspects.\footnote{31} As section 5 below describes, data protection represents one approach that can be connected to the notion of informational privacy. It is however important to note that whilst data protection represents an important legal concept that is linked to privacy it is not the only one.\footnote{32} It is entirely possible that where it does not apply (i.e. because the use of personal data is not involved), other legal and ethical approaches linked to privacy may be relevant (especially when privacy is considered from a wider perspective).\footnote{33} As section 4 of this document discusses, this involves other privacy linked approaches and doctrines including notably those developed by the ECtHR under Article 8 ECHR.

### 3.1.3 Privacy and Surveillance – The need for a wide conception of privacy

Privacy is also arguably linked to the idea of surveillance. This is particularly true for those who hold a wide definition of privacy i.e. related to the concept of ‘being left alone’ or not ‘being steered’ and not just a narrow one i.e. relating to ‘informational privacy’ (see 5 below).’ Surveillance, (for example CCTV cameras) may be considered intrusive by individuals even though they do not collect any information that is already not in the public domain. This is because despite the fact that such measures do not use private personal information they are still capable

\begin{footnotesize}
\begin{enumerate}
\item H. Nissenbaum, (1998).
\item Personal data has a specific legal definition defined in Directive 95/46/EC Article 2(a) as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"
\end{enumerate}
\end{footnotesize}
of imposing upon individuals in a psychological sense.\textsuperscript{34} Individuals may for example alter their behavior (even when such behavior is legal). Looking at such matters in terms of purely informational privacy would not be sufficient to understand the harms that unnecessary surveillance can bring about.\textsuperscript{35} The need to view surveillance matters in a way that goes beyond a simple vision of privacy as a form of informational control is described well by Nissenbaum.\textsuperscript{36}

“As disturbing as the practices of public surveillance are, they seem to fall outside the scope of predominant theoretical approaches to privacy, which have concerned themselves primarily with two aspects of privacy – namely, maintaining privacy against intrusion into the intimate, private realms, and protecting the privacy of individuals against intrusion by agents of government. Philosophical and legal theories of privacy offer little by way of an explicit justificatory framework for dealing with the problem of privacy in public. Indeed, with only a few exceptions, work within these traditions appears to suffer a theoretical blind spot when it comes to privacy in public, for while it has successfully advanced our understanding of the moral basis for privacy from some of the traditionally conceived threats, such as violation of the personal sphere, abuse of intimate information, protection of the private individual against government intrusion, and protection of, say doctor-patient, lawyer-client and similar special relationships, it has not kept abreast of the privacy issues that have developed in the wake of advanced uses of information technology.”

A recognition of the the harms that surveillance practices can produce for privacy in the broad (i.e. not purely informational) sense, is important in the context of the FORENSOR project. This is because the expected use of the FORENSOR prototype may often involve the recording of images or videos of individuals in public locations. Furthermore it is likely, given the quality of expected recordings, that images may often not include aspects of individuals that are recognizable or linkable to a specific individual. Even in such a case however the concept of privacy in a broader sense may still be relevant. This is because individuals may not want to be monitored, even if in a public place, or even if personal information that can be specifically linked to them as individuals is not be recorded. Individuals may for example feel disturbed at the prospect that the police could be alerted to their presence (even if they are not taking part in illegal activity). The possibility of being monitored may induce people to behave differently in areas that are being monitored or even avoid going to those areas at all. In this sense the existence of surveillance systems are capable of exerting ‘steering effects’ upon individuals and should thus be considered from the perspective of privacy, even where they do not strictly pose a threat to individual privacy in the narrower ‘informational sense’. This will idea will be reflected upon further in a legal sense in section 4 where the difference between data protection (i.e. related to privacy in the narrow

\textsuperscript{35} S. Gutwirth, (2002)
\textsuperscript{36} H. Nissenbaum, (1998).
sense) and more general provisions such as Article 8 of the European Court of Human Rights (which relates to privacy in a ‘broader sense’).

3.1.4 Data Protection as an Approach to Promote Individual Privacy

Data protection approaches lay out rules and conditions for the processing of personal data (i.e. data that can be related to individuals).\(^{37}\) It is thus linked to privacy in that it can reduce the chances that individual data is misused with consequent harms to individual autonomy (see above).\(^{38}\) Data protection may however differ in some regards to other approaches linked to the concept of informational privacy in that it is not primarily concerned with harms that can occur through the misuse of data but rather solely with the misuse of data itself. Data protection is concerned with promoting the correct use of personal data, i.e. ensuring that personal data is collected only where a valid legal ground exists and processed in accordance with a number of important principles. Data protection principles can thus be engaged even where there is no demonstrable harm to individual privacy. This is important for those who intend to process personal data as it means that breaches of data protection principles can occur even where no individual has complained of harms to his or her privacy.

Data protection only applies where personal data is involved i.e. data that can be linked to a specific individual. Where the data processed is not personal, data protection law does not apply (though other approaches related to the broad concept of privacy may still be of application).\(^{39}\)

3.2 The need to foster security as a counterweight to privacy.

3.2.1 A right to privacy can not be absolute

States and societies have many duties with regards to their citizens and participants. Whilst the protection of privacy (in its various forms) is important it represents but one of the duties states should try to fulfill.\(^{40}\) Other prominent duties relate to the need to protect the life and property of citizens, to prevent disorder to ensure that justice occurs where individuals have been the

---

\(^{37}\) P. De Hert and S. Gutwirth, 2006


\(^{39}\) The definition of

\(^{40}\) D. Klitou, *Privacy Invading Technologies and Privacy by Design* 2014). p21 -p27
victim of criminal activity and to protect national security.\textsuperscript{41} In a pluralist society it is not possible to offer such things in an absolute manner to all individuals all of the time. This is because the different individuals and different groups will often have competing interest and desires, including different visions of how society should operate. In this pluralistic reality that most of us inhabit, privacy is just one value that must be considered alongside others such as security and the need for public order. If any of these values were to be given an absolutist weight the result would be a dystopian chaotic society that would not be able to function.\textsuperscript{42} This is no less true with regards to the value of privacy. In order to provide security the state will likely have to take measures that may infringe upon the privacy of individuals.\textsuperscript{43} The state security structure may have to collect data or conduct acts of surveillance to prevent acts of terrorism for example. Individuals may have to restrain certain behaviors that they may have otherwise wanted to have engage in e.g. drink driving, smoking in public places, or having to provide personal details when booking airline tickets. All such measures impinge upon the privacy of individuals, but do so for good reasons. As a result of this situation of competing values and rights it is often necessary for the state to strike a balance in order to uphold the rights of all groups in society to the greatest extent.\textsuperscript{44} Various thinkers and philosophers have considered this issue and many have come to the conclusion that it is necessary to infringe upon individual prerogatives only where there is a good reason to do so. Kant’s categorical imperative is perhaps the most famous example.\textsuperscript{45} Others such as Rawls came to the conclusion that a society should only impinge on the rights and freedoms of certain individuals when it must do so to protect the ideas of others.\textsuperscript{46}

### 3.2.2 Infringements upon privacy should be of a proportional nature

Whilst it may be intuitively obvious to most individuals that the state will, from time to time, have to infringe the rights of some to protect those of others, the question remains as to how it should make such a decision on a case-by-case basis. Which values should take priority and how should it weight competing claims. One idea that is often given prominence in both ethical and legal thought is the idea of ‘proportionality’.\textsuperscript{47} It relates to the idea that the rights of some may be

\textsuperscript{41} The protection of security for example receives fundamental rights status through Article 6 of the Charter of Fundamental Rights and Freedoms of the European Union Other duties such as the right to healthcare are accepted in some societies but not others. For more on this discussion see: N. Daniels, Justice, health and healthcare, American Journal of Bioethics, 1,(2) (2001) pp. 2-16

\textsuperscript{42} A. Etzioni, The Limits of Privacy (New York: 1999).

\textsuperscript{43} For a critical view on such an idea see: M. Neocleous, Security, Liberty and the Myth of balance: towards a critique of security politics, Contemporary Political Theory, 6,(2) (2007) pp. 131-149

\textsuperscript{44} D. Klitou, (2014)


\textsuperscript{46} J. Rawls, A Theory of Justice (MA: 1971).

\textsuperscript{47} For more on the concept of proportionality, especially from a legal perspective see: K. Moller, Proportionality: Challenging the Critics, International Journal of Constitutional Law, 10,(3) (2012) pp. 709-731
infringed if, in doing so the aim is to bring about a situation where the harm that would be caused would be less than if the infringement never occurred. Such an idea is useful because it allows one to assess where certain actions are necessary or not. Using the examples given above for example one might say that it is relatively straightforward to argue that the harms (in terms of personal autonomy) in preventing individuals from drink driving are less than the harm that would be caused by allowing people to drink drive at will (i.e. loss of life and injury). A similar argument could be made for smoking in confined public spaces. The same idea can often be applied to security measures that may infringe upon personal privacy. In some instances the measures in question may be proportional. Imagine for example the use of cameras or other surveillance measures in airports or other obvious terrorist targets. Imagine the use of CCTV in areas that have been riddled by crime that has involved numerous victims. In such instances the harms to personal privacy that may be perceived by some individuals are arguably not sufficient to render the aims behind the security measures disproportionate.48 In such instances was the state not to act in order to protect human life and limb it would arguably not be meeting its duty towards its citizens of providing security and protecting life and property.49 On the other hand however some security measures may be questionable and clearly not proportional given that the aim they intend to achieve is not proportional when one takes into account the harms to privacy that are likely to occur. This may for instance include grave violations of privacy that are intended in order to deal with minor threats to security or order or petty criminality.

One important aspect of the proportionality approach towards conflicting rights and interests is that it demands that there must be a good reason for the state to infringe upon the rights or interests of an individual or group in society.50 Where such a good reason does not exist i.e. representing the need to act to protect important rights of others, it will not be acceptable to act in a way that harms the rights or interests of some. The need to balance the privacy and security interests of various groups and individuals in society means that security measures that infringe upon individual privacy are not acceptable unless they really are intended to meet a need that is relating to protection the rights and interests of others. Where such a justification does not exist, infringement of individual privacy would not be acceptable.

49 D. Klitou, (2014)
3.3 Relevance of the privacy v security paradigm for the FORENSOR project

The often competing nature of claims related to privacy and security are obviously relevant in the context of the FORENSOR project. FORENSOR by its very nature is something that poses a risk to privacy. Whether this be in the narrow informational sense or the broader sense this is something that is important to consider. With regards to the former, it is important to discern if, where and how FORENSOR will make use of information pertaining to identifiable individuals. Where it does it will be necessary to comply with frameworks that are established in order to protect personal data (the most important are described in the following section concerning legal approaches). It is important however to recognize that privacy need not only relate to information concerning specific individuals but can also be thought of in a wider sense. Surveillance activities that are not likely to use individual information may still exert psychological pressure upon individuals that may be capable of altering their behavior. Individuals may not feel comfortable acting in a way that they may have otherwise have done so if they feel they are being monitored or if they feel that their simple presence may draw unwanted attention. Such aversion may even be the case where people are not committing illegal activities but for one reason or another may not want people to be aware of their presence in a certain place at a certain time.

Such potential infringements on personal privacy (whether it be in the narrow informational or broader sense) are not always unacceptable however. This includes potential uses in incidences relating to crime and security for which FORENSOR is intended. Depending on the level of infringement of privacy that occurs and the intended use, the deployment of FORENSOR devices may be acceptable in certain contexts. The concept of proportionality provides a useful way of judging when such infringements may be acceptable. In terms of possible infringements upon privacy imagine for example the difference between cameras viewing private property or public areas. Imagine also the difference between a surveillance system that is activated by all passers by and a surveillance system that is only activated by certain events that are more likely to correlate to criminal activity. Imagine also the aim of the measures in question. Are they intended to tackle serious crime (e.g. Drugs smuggling or other organized crime) or are they intended to tackle petty criminality (e.g. dropping of litter or illegal parking)? In deciding upon whether a potential use would be acceptable it would be necessary to take all such factors into account.
4 Privacy (in the broad sense) in law

This section of the document follows on from the discussion of privacy in the ethical sense in the previous section. The aim will be to illustrate how the law recognizes rights to privacy in the broad sense i.e. ‘as a right not to be steered’.\(^{51}\) This will first involve highlighting prominent sources of privacy rights in international and European law with a focus on the European Convention of Human Rights given its widespread application and binding nature for almost all states in Europe.\(^{52}\) The focus will be on the applications of such legal principals to potential instances of surveillance. In particular, the aim will be to demonstrate how the European Court of Human Rights is likely to take into account privacy issues related to surveillance practices and consider them in the light of other important interests such as maintaining public order and the prevention of crime. In doing so this section will illustrate how principals discussed in section 3 are balanced against each other using the concept of proportionality. This section will furthermore discuss how the concept of ‘privacy by design’ may play a role in making the use of surveillance technologies more ‘proportional’ and thus less likely to be deemed an infringement of privacy when used in practice. At the end of this section these concepts will be discussed in the light of the FORENSOR project with the intention of highlighting the key principles that should be born in mind throughout the project and in the privacy impact assessment which will be conducted in deliverable 2.2.

4.1 Prominent protection for privacy found in international treaties

At the international level, the right to privacy is protected by Art 12 of the Universal Declaration of Human Rights (1948). Whilst this is non-binding on the legal systems of individual states it is non the less of considerable symbolic importance:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Art 17 of the International Covenant on Civil and Political Rights (1966), i.e. which signatory states are themselves bound to uphold offers protection in terms of privacy

\(^{51}\) The term ‘steering’ was coined by Gutwirth in describing the power of societal forces (including the sate) to shape not only the behavior of individuals but also their thoughts. See: S. Gutwirth, (2002)

stating:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

4.2 Privacy at the European Level

The European Union’s Charter of the Fundamental Rights (CFR) which entered into force after the enactment of the Lisbon Treaty. It explicitly recognizes a fundamental right to privacy in article 7 under the notion ‘respect for private and family life’, stating: “Everyone has the right to respect for his or her private and family life, home and communications.” The application of this is however restricted to the activities of European Institutions and the implementation of EU law. In areas that are not related to these, this will be of little concern. The application in the field of criminal law is thus likely to be limited given that the EU’s competence on laws relating to national criminal justice related practices are limited.

Of more direct importance is the European Convention on Human Rights (the ECHR). It has more direct relevance than the CFR for two reasons. First it is applicable to all Member States of the Council of Europe. This is an organization that encompasses nearly all the states of Europe in a geographical sense and thus goes beyond the Membership of the EU itself (the Member States of the EU are obliged to be member of the CoE and signatories to the ECHR). Furthermore the rulings of the European Court of Human Rights (the ECtHR) are binding in a general sense upon the legal systems of the Member States of the CoE. This means that they are in reality capable of having

53 This is described by Article 51(1) of the EU Charter which states: “The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers. For more see: F. Fontanelli, The European Union’s Charter of Fundamental Rights two years later’, Perspectives on Federalism, 3,(3) (2011) pp. 22-47

54 Ibid., In ERT case the Court found that ‘EU human rights law applies to Member States not only when they are implementing EU law, but whenever they are “acting within the scope of Community law.” If this is the criterion, then the Charter applies not only when States directly implement an EU norm, but also when they derogate therefrom, maybe even when their acts may simply affect Union law at large. The external limits of the Charters’ effects are still to be delineated, admittedly, and will probably remain unresolved unless the Court of Justice of the EU (CJEU) sets up a new test to identify them”


D2.1 - Report on the Data Protection, Privacy, Ethical and Criminal Law Frameworks

direct effect, giving rise to not only to the possibility for damages or other reparations for individual complainants, but also that they set precedents for the future interpretation of national law.

On privacy article 8 of the ECHR states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4.3 The ECHR and privacy the context of surveillance technologies and practices

Article 8 ECHR has been applied by the court in an enormous variety of situations. These include in areas related to both the narrow 'informational' concept of privacy and in the broader privacy 'as freedom from steering' sense as described in section 3 of this document. With regards to the ECHR to surveillance systems. The ECHR has for example stated (in the P & J v UK case) that:

“There are a number of elements relevant to a consideration of whether a person’s private life is concerned by measures effected outside a person’s home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any

59 Case of PJ & H v United Kingdom (Application Number 0004478/98 2001) For more discussion of this case in the context of surveillance matters overall see: R. Macroy, Regulation, Enforcement and Governance in Environmental Law 2014). p297
intrusive or covert method (see Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V).17 “

The court therefore accepts that in general, CCTV and other surveillance systems in public places are capable of engaging individual rights under Article 8 ECHR, i.e. a right to private and family life. This does not however mean that such ‘engagements’ can automatically be equated to violations of Article 8. This is because Article 8 contains a qualification in paragraph (2). This qualification takes into the account of the fact discussed in section 3 that it may be necessary on certain occasions to take measures that fight crime, protect individuals and maintain public order. In implementing such a ‘qualification’ the ECtHR uses the concept of ‘proportionality”, also discussed in section 3. The ECtHR is its decisions has shown that the qualification permitted in article 8(2) allows individual rights under article 8 to be engaged in appropriate circumstances (including those related to surveillance practices). 60 This are:

(i) When a measure has a valid aim or acceptable goal: i.e, national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others
(ii) When the measure is described in law
(iii) When it can be considered necessary in a democratic society.

In terms of an ‘acceptable goal”', erecting surveillance measures may therefore be acceptable where they are ‘intended to prevent disorder or crime’ as permitted by Article 8(2) ECHR. In terms of requirement (ii) above, the court usually looks for existence of overt laws or powers, usually in the form of legislation that grant local authorities or the police the power to engage in the type of surveillance in question. Laws of this type do not exist on the European level but on the national or even local level. It is therefore important to be aware of the local situation that exists in terms of the law in force in the particular jurisdiction concerned. Such laws can vary considerably. An example of such a situation is shown in Annex III to this document concerning the legal situation applicable in Chiusi village (relevant to one of the use case scenarios). The existence of such laws is not itself sufficient to guarantee that the use of surveillance methods (such as cameras or CCTV)

60 Relevant cases from the perspective of surveillance in issues include Case of S. and Marper v the United Kingdom (Applications nos. 30562/04 and 30566/04), Case of MALONE v. THE UNITED KINGDOM. (Application no. 8691/79), Case of Peck v the United Kingdom (Application No. 44857/98) For more discussion on the rulings of the ECtHR in the context of surveillance issues see:V. Kosta, Fundamental Rights in EU Internal Market Legislation 2015).P92
will not be a violation of article 8.\textsuperscript{61} This is because as (iii) describes above, such measures must also be ‘necessary’. In its case law on this matter the court usually concerns itself with the question of the ‘proportionality’ of the measures in question. In deciding whether a measure was proportional or not the court will look at what the measure in question is attempting to achieve and make a judgment on whether the harms that may occur in terms of personal privacy may justify the measure in question.\textsuperscript{62}

In deciding whether surveillance measures such as surveillance local authorities must therefore not only ensure that there the measures in question are authorized in law (e.g. statute) but that that are both necessary and proportional in the particular context concerned.\textsuperscript{63} This means that in order to decide whether the utilization of a particular system of surveillance is legal or not it is necessary to look at the particular context in question. In performing this analysis it will be necessary to look at aspects such as;

\begin{itemize}
  \item The problem which is being addressed (i.e. the seriousness of the crime be tackled)
  \item The level of invasiveness (e.g. is the measure to be taken in busy public areas or private property)
  \item The level of foreseeability for those who might be involved (i.e. is there warning of the measures in question?).
  \item Have procedural or technological measures been taken in order to reduce potential harms to individual privacy.
\end{itemize}

The nature of the points raised here indicates the contextual nature of the decision that must be made on particular surveillance practices on a case-by-case basis. This contextually means that it is not possible to know whether a particular surveillance practice would constitute a violation of Article 8 ECHR simply by looking at one of the aspects raised above. This means that for example one can not simply assume that such practices are legal by virtue of the fact that legislation exists that seems to permit such practices. Nor can one deduce legality by the fact that the particular technology employed is designed in such a way so as to to reduce the impact on individual privacy i.e. the implantation of so called ‘privacy by design’\textsuperscript{”} (PBD) (see discussion on privacy by design below) or even because the measures intended are genuinely employed to tackle issues related to crime and security. What is rather needed is an analysis that taking into account the particular

\textsuperscript{61} R. Weber and D. Staiger, (2014).
\textsuperscript{62} K. Moller, (2012).
\textsuperscript{63} Marper v UK
context, considering all of these elements together. Requirements relating to proportionality may also exist explicitly at the national level. Examples of this from the perspective of the Portuguese constitution are shown in Annex IV.

4.3.1 The contribution of privacy by design and privacy enhancing technology to the question of proportionality.

Whilst not being the sole factor to be considered above, the concept of PBD (i.e. the existence of measures to reduce the potential impact on individual privacy) allows for an important possible contribution in terms of privacy enhancing technologies. The existence of such factors in the development and implementation of surveillance technologies is a factor that can be taken into account in determining the proportionality of a potential deployment.\(^{64}\) Where such techniques have been employed, the use of a surveillance system is more likely to be considered ‘proportional’ in a wider range of contexts. Such techniques could inter alia for example involve ensuring that images or recordings were taken only when absolutely necessary or that would only be activate where activity likely to be criminal in nature was taking place. These are factors that are likely to be of relevance to the FORENSOR project and will be discussed further in 4.3.2.

The concept of PBD is particularly important in the design and development phases of technological projects related to surveillance.\(^{65}\) If such a concept is not implanted at this stage it will be too late to build them in later. If PBD is not considered at the design stage the result may effectively be a need to depend more on the other aspects described above when determining proportionality (given the application of the Article 8 ECHR as discussed above). This may mean for example the restriction of surveillance practices to contexts that only involve severe criminality or to settings where intrusion upon personal privacy are likely to be limited (i.e. in busy public places and not in more secluded or private settings). The de facto effect therefore of not correctly implementing PBD may be a reduced possibility of deployment in terms of the range of contexts in which the surveillance system in question can be used in.\(^{66}\)

4.3.2 General privacy approaches – key points for the FORENSOR project

The proposed FORENSOR prototype represents a technology that will be used for surveillance

---

\(^{64}\) K. Moller, (2012); D. Klitou, (2014)
\(^{66}\) D. Klitou, (2014)
purposes. As such, the FORENSOR device, when used for such purposes will be capable of infringing on the privacy of individuals. Such infringement will occur whether such surveillance occurs in busy public areas, secluded public areas or private property (though the infringement will be of a much graver nature in the last case). Whilst such actions may be infringements of privacy, they may not, depending on the context in question be illegal. This is because in many contexts such surveillance measures may be necessary and proportional in order to address issues of crime and public order. Article 8 ECHR recognizes this by offering a qualification to its general protection inter alia for measures that are intended to prevent crime. As discussed above, this does not mean that the mere fact that where a ‘Forensor like’ device is used in order to detect or prevent crime it will automatically be legal. This is because the use of such a device in particular context in would have have to meet the conditions of having being both described in law and being necessary and proportional. The FORENSOR project itself is not in a position to address the first of these issues – that is something that only national and regional legislators can address. Once again the particular context in question is also something that the FORENSOR project will not be able to influence – that is the choice the the particular law enforcement agency ‘on the ground’ to decide upon i.e. on the particular local conditions may require the deployment of the device. Where FORENSOR as a research project is however able to make a realistic difference to this question of proportionality, and therefore by extension legality is by making the design of the device in question as ‘privacy friendly’ as possible. This need prevents both an opportunity and an imperative to incorporate PBD in the design and development of the FORENSOR prototype. Through doing so (e.g. by designing the device in a way that it only records activity at certain times or activity that is highly likely to be only of a criminal nature) the chances are higher that the use of the device in a particular circumstance will be deemed as being ‘proportional. This is important given that it is something that will be paramount in the minds of the police, prosecutors and investigative judges when they are deciding upon requests to deploy the device. A failure to do so would run the risk that the FORENSOR device could only be used in the most grave of contexts (i.e. involving very serious criminality) and would reduce both its appeal and potential uptake.

5 Data Protection – A Prominent Legal Approach Concerned with Privacy in the Informational Sense.

This section will explore the potential impact of data protection approaches on the FORENSOR project. Such approaches represent the most important example of legal approaches that are concerned with protecting informational forms of privacy (as discussed from an ethical and theoretical viewpoint in section 3). Data protection approaches may be relevant to the FORENSOR
project when it conducts research that may involve particular individuals e.g. who might be filmed in use case scenarios.

Data protection is conceptually different that the privacy approaches discussed in section 4 most notably because its engagement does not depend on demonstrating that harm has occurred to a particular complainant (i.e. an infringement of privacy, harm to reputation or something similar). Rather data protection approaches present a number of rules and principles that must be adhered to in all cases of data processing. Not following such rules and principles will immediately lead to a data protection breach which not only gives rise to legal action against the processor of personal data but also the possibility of damages for the data subject involved. Data protection frameworks are overseen by national authorities in each Member State of the EU. These often have the power to investigate the data usage of organizations so as to ensure that they are complying with the data protection framework in place. There is therefore not only an important moral imperative to respect data protection rules and principles, but a practical one also.

5.1 FORENSOR and personal data

The EU’s data protection approach applies when personal data is being processed. As is discussed further below in section 5.3, personal data is defined in Directive 95/46/EC (Article 2) as “any information relating to an identified or identifiable natural person”. Where data can not be linked to a specific individual it will not be classed as ‘personal data’ and thus not enjoy the protection of the EU’s data protection framework. At the time of writing it is still not certain whether a FORENSOR prototype would involve the use of personal data. This is because the quality of the images captured by the device is not likely to be sufficient to identify individuals e.g. through facial images or license plate numbers on cars. Given that this is not yet certain it is wise to consider the potential impact of data protection legislation should this happen. Furthermore, the development of the FORENSOR prototype is is likely to involve trials and experimentation that may involve the use of personal data. This may for example occur where images of volunteers are recorded for modeling purposes. Research for the FORENSOR project may inter alia involve the use of conventional filming equipment for modeling purposes. It is important to consider the application of data protection legislation to both of these contexts (i.e. the use of a FORENSOR prototype for matters of criminal investigation and the use of personal data for research purposes in the FORENSOR project). As the sections below indicate, the potential application of DP law is different for each type of activity and should be considered carefully.

---

67 P. De Hert and S. Gutwirth, 2006
5.2 The Council of Europe’s data protection approach

The Council of Europe (CoE) adopted, in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No 108) with an additional protocol regarding supervisory authorities and transborder data flows (No 181). The Convention applies to both private and public sectors (Article 3(1)), including police and judicial issues, unless a member state opt-outs (Article 3(2)). Despite being supervised by the CoE these conventions are open not only to Member States of the Council of Europe but also to any other state that wishes to join them. In addition to the convention the CoE has also adopted a number of recommendations directed at Member States concerning data protection.

5.3 The EU’s Data Protection Approach

The EU’s data protection approach is particularly important given that it has created law that is binding in all the Member States of the EU. This means that the principles and rules it creates are capable of giving rise to both legally enforceable obligations for data controllers/processors, and rights for the data subjects concerned. EU rules concerning data protection are found both in primary law (i.e. in the EU treaties) and in secondary law (legislative initiatives such as directives and regulations). The former represent general principles and commitments that often form the legal basis for more precise legislative and judicial initiatives. The latter represent more complex binding rules that can be applied in a wide range of circumstances. The most important elements with regards to data protection are outlined in both below.

5.3.1 Fundamental Commitments in Primary Law

The European Union’s Charter of the Fundamental Rights (CFR) which entered into force after the enactment of the Lisbon Treaty. It explicitly recognizes a fundamental right to data protection with Article 8 stating:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.
In addition to the CFR the EU treaties themselves (which amount to primary law in EU terms refer to the need to protect personal data (Article 16 of Treaty on the Functioning of the European Union (TFEU) and Art 39 of Treaty on the European Union).

5.3.2 EU Legislative Initiatives (Secondary Law)

Legal declarations such as those above represent general requirements and principles that applies in the interpretation and application of European Union law. Of more practical importance are the specific legislative initiatives that the EU has taken with regard to data protection. Most of these take the form of directives which have been transposed into national law. This process of transposition allows for some variation along national lines whilst preserving the essential context of the directive concerned. The most important are:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the 1995 Data Protection Directive);


Other more specific legislative initiatives that will like have an important relevance for the FORENSOR project include:

- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (i.e. former 3rd pillar, see infra, at 3.2.2.2.2), and

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (i.e. lying down data protection rules applicable only for the EU institutions and bodies).
5.3.3 The main regulatory actors concerned with privacy and data protection.

Although the Directive 95/46/EC is a European legislative initiative, the main regulatory bodies it foresees for the enforcement of data protection law are established at the national level. These take the form of National Data Protection Authorities (sometimes known as ‘National Data Protection Commissioners’). There existence is mandated by by Directive 95/46/EC which requires that each Member State maintain a national institution upon its territory responsible for the oversight of data protection issues.\(^{69}\) National authorities should, in principle, have the power to power of “investigation, of intervention and of engagement in legal proceedings) and 28(4) (power to hear claims)”, though not all national authorities use these powers effectively.\(^{70}\)

At the European level there exists the European Data Protection Supervisor (the EDPS).\(^{71}\) The role of the EDPS is to supervise the EU institutions, bodies offices and other agencies. The EDPS may therefore be contacted for queries concerning European research projects but whilst he EDPS has a role in fostering co-operation and consultation between national authorities, it has no powers of oversight or control.

5.3.4 Data Protection Requirements of Potential Application to the FORENSOR project.

This section describes key principles that must be adhered to in all instances of data processing, including processing of data that may occur in the context of the FORENSOR project.

5.3.4.1 Data Processing Must Have a Legal Basis

Directive 95/46/EC in Article 6(1) demands that personal data must be ‘fairly and legally' processed. In order to comply with such requirements personal data may be processed for one of the following reasons (described in article 7).

(i) the data subject has unambiguously given his consent; or


\(^{70}\) Ibid P22

\(^{71}\) Established by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
(ii) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(iii) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(iv) processing is necessary in order to protect the vital interests of the data subject; or

(v) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(vi) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

With regards to research within the context of the FORENSOR project the most relevant legal base is (i) as described above i.e. the consent of the data subject. Consent will therefore be necessary where research subjects are to be used to provide personal data for the purposes of research within the the project. Such consent should be provided in an unambiguous manner by those involved.

The situation described above does not however apply to the theoretical use of a FORENSOR prototype by Police for the detection of criminal activity. Such use is exempted from the field of application of Directive 95/46/EC by Article 3(2) which excludes its application to personal data being used in connection with police and criminal justice activities. In addition, Council Framework Decision 2008/977/JHA (described above) only applies in cases where personal data that is being used for matters connected to crime and security is transferred from one Member State to another.72 Where this is not the case, neither this, nor any other of the EU’s data protection initiatives will apply. The use of data in such contexts therefore does not have to comply with EU data protection requirements.

The lack of application of data protection law in the contact of criminal proceedings does not however mean that the use of personal data will be beyond legal scrutiny. This is for two reasons.

(i) National laws on data protection may still apply in certain contexts. Despite the fact that they are not required to by Directive 95/46/EC to some member states have decided to apply their domestic legislation to police and criminal justice activities in certain contexts. Whilst Council Framework Decision 2008/977/JHA does not apply to the use of personal data on a purely national basis, it does not prevent Member States from creating their own legal requirements on such issues. Such requirements may exists, but should be looked at on a state-by-state basis.

(ii) Laws pertaining to privacy will still apply (these were discussed in greater detail in section 4 above). This includes requirements (such as those described by the ECtHR) concerning the necessity, legality and legal basis (i.e. having a legitimate aim of surveillance activities.

5.3.4.2 Sensitive data

Sensitive data is a category of data created by Directive 95/46/EC for which stricter requirements apply in terms of the legal base that is necessary. At present it does not appear likely that the FORENSOR project will involve the processing of sensitive data. Furthermore, given the type of prototype envisaged, it does not seem likely that it would involve the use of sensitive data even in the context of a police (or similar) investigation. In order to fully consider their potential application, the following text briefly describes the properties of sensitive data and the requirements that pertain to their processing.

Sensitive data is data that can reveal aspects such “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and concerning health or sex life” concerning a particular individual. In principle the processing of such data is forbidden. Article 8(2) however lists certain exceptions. These are:

- Where the explicit consent of the individual concerned has been received.
- Obligations in the field of employment law,
- The protection of a vital interest of the data subject in a situation where the subject in question is incapable of giving his consent.
- For the legitimate activates of a foundation, association or any other non-profit body.
- For the purposes medical diagnosis or treatment (including preventative treatment)

---

74 Article 8(1)
of a medical condition.

Where none of the above conditions are met, processing of sensitive data may be permitted where such processing would be in the public interest and a number of conditions are met. These involve that the measures in question be described in legislation and that certain measures be taken in order to ensure the security of the data in question. Given that specific legislation is required, such an option is not likely to be available to the FORENSOR project should it have to process sensitive data.

5.3.4.3 Data processing must adhere to certain processing principles

The following principles are described in Article 6 of Directive 95/46/EC and must be applied in all instances of processing of personal data to which the directive is applicable. Such principles will be of relevance to FORENSOR, especially in relation to research that uses personal data.

(i) **Data minimization** - This principle acts to restrict the use of personal data, even where there is a valid legal basis for its collection. Data must be collected for specific, explicitly defined and legitimate purposes and not further processed in a way incompatible with those purposes. In addition, data should only be retained only for as long as is necessary to fulfil that purpose. Afterwards it should be deleted.

(ii) **Data quality** - Measures must be taken to ensure the personal data is of satisfactory quality. This includes ensuring that the data is adequate, relevant and not excessive in relation to the purposes for which it is collected and processed. In addition data must be accurate and, where necessary, kept up to date.

(iii) **Data anonymisation (where possible)** - In principle data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Where possible data should be anonymized.

(iv) **Data security** - Appropriate technical and organizational measures should be

---

75 Article 6(1)(b)
76 Article 6(1)(c)
77 Article 6(1)(c)
78 Article 6(1)(e)
taken so as to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. This is particularly important where the processing involves the transmission of data over a network.\footnote{Article 17}

(v) **Confidentiality of data processing** - Directive 96/46/EC does allow personal data to be processed by any other person that the data controller unless they are instructed by the controller to do so or there exists a legal basis for such processing.\footnote{Article 16 states that “any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.}

(vi) **Notification Requirements** - A data controller must notify the national supervisory authority before carrying out any wholly or partly automatic processing operation.\footnote{Article 18(1)} This requirement may not apply in certain instances however, this includes where an in-house data protection official has been appointed.\footnote{Article 18(2)}

### 5.3.4.4 Rights of the Data Subject

Where applicable, Directive 95/46/EC, provides that the data subject should have a number of important rights in national law. These are;

- The right to be informed of the processing of his or her personal data;\footnote{Ibid}
- The right to access his or her own personal data;\footnote{Article 12(a)}
- The right to rectify incorrect personal data;\footnote{Article 12(c)}
- The right to object to processing on legitimate grounds;\footnote{Article 14}
- The right not to be subject to an automated decision that will be used to evaluate certain personal aspects relating to the data subject.\(^{87}\)
- The right to a judicial remedy and the right to receive compensation where there has been a breach of data protection rights.\(^{88}\)

Of particular relevance to the FORENSOR project are the right to be informed of data processing and the right to access any potential data. The former right is linked to the concept of consent because without being informed it is in reality impossible to give consent. Such a right is particularly important in the research phase of FORENSOR where individuals have a right to know that that they are in an area where filming (i.e. for research purposes is occurring). Such information is needed to avert individuals to the possibility that their personal information (i.e. in the form of visual images) may be being collected and processed. In the context of the FORENSOR project, such a requirement may mean that signs or notices are needed in areas where prototypes are being tested or simulations are being made in order to warn individuals that their personal data may be being collected and processed.

### 5.4 Transferring data across borders

The Data Protection Framework is also important in the regulation of the cross border transfer of data. This is logical given that one of the motivations behind the directive was to facilitate internal trade that was dependent upon the use of personal data. EU data protection draws a distinction between transfers of data within the EU and transfers of data to third countries i.e. outside the EU.

#### 5.4.1 Within the EU

As described above, one of the rationales of Directive 95/46/EC was to remove borders to the safe transfer of personal data within the EU and thus facilitate the development of the single market.\(^{89}\) The general rule regarding the transfer of personal data across national borders is that it is permissible within the EU or with other countries outside the EU that afford the same level of

---

\(^{87}\) Article 15  
\(^{88}\) Articles 22 and 23  
data protection rights. Directive 95/46/EC establishes that data may be transferred freely between member states, in Article 1:

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

The main principal at play is that within the EU all Member States should have implemented the requirements of Directive 95/46/EC and should thus constitute environments where the respect for privacy and personal data is guaranteed in law. Prohibiting transfers within the EU for such reasons is therefore not permitted. Given this, the rules that apply within the national data protection of a particular Member State and intended to apply to data transfers within that Member State should also apply to transfers to other EU Member States.

5.4.2 Outside the EU

The principal provisions of Directive 95/46/EC is enacted not only in the EU but also in the countries of the European Economic Area (EEA). This include Iceland, Liechtenstein and Norway. For these states the same rules apply as intra-EU transfers of personal data. For transfers outside the EU however, a more stringent level of regulation is demanded.\(^\text{90}\) The logic behind this is that countries outside the EEA may not have the same level of data protection in their law as the countries of the EEA, including those described within Directive 95/46/EC (described above). For this reason Directive 95/46/EC requires that, in general, transfers to countries outside the EU be forbidden. There are however some exceptions to this principle. The most important (in the case of the FORENSOR project) of these is where the express consent of the data subject has been secured.\(^\text{91}\) In order to utilize this option, it is necessary to explain to all data subjects involved that their data will be transferred to a state outside the EEA and that such a transfer is to an area where EU rules on data protection do not apply. Such consent must be secured even if a valid legal ground already existed for the collection of the data in the first place.

\(^{90}\) Ibid.,

\(^{91}\) This and other exceptions are described in Article 26 of Directive 95/46/EC
Another option that is available is the use of the so called ‘Safe Harbour’ derogation. The concept of ‘safe harbor’ applies to instances where the EU Commission has publically made a decision that a particular state has a level of data protection law that will guarantee protection to the level of that found under 95/46/EU. This occurred where the states in question had agreed upon a list of safe harbor principles for the correct processing of personal data. These agreements would then be available for data processors in the state in question to sign up to and adhere to before receiving personal data from the EU. The EU Commission had granted recognition to the safe harbor principles outlined by Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US Department of Commerce. The existence of such a decision meant that personal data could be transferred to processors from an EU or EEA country to that third country without any further safeguard being necessary.

The ‘safe harbour’ system was however called into question in the recent Schrems case (which involved the cross border transfer of data by Facebook). In that case the European Court of Justice ruled that the current ‘safe harbor’ arrangements in place with the United States were not sufficient to grant the level of protection that Directive 95/46/EC envisages. As a result of this the current safe harbour agreements should be considered invalid. The EU Commission is currently revising its safe harbour agreements to take into account the ruling of the ECJ in Schrems. Until this occurs however the 'safe harbour’ exception should be considered unavailable, meaning that one of the other exceptions in Directive 95/46/EC should be utilized (e.g. obtaining explicit consent).

5.5 Examples of data protection law in various member states of the EU.

The main legislative initiative in force is at present is Directive 95/46/EC described above. The choice of Directive as the legislative instrument in this context means that the EU legislation is not

---

93 For Israel for instance the relevant decision was Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (2011/61/EU)
94 The EU Commission has made more guidance on this matter available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
95 Maximillian Schrems v Data Protection Commissioner, (2015), Case C-362/14
directly binding but requires Member States to create national legislation reflecting its requirements. Whilst this means that the main elements of a directive are given force through a process of ‘transposition' in EU Member State legal systems, it does not mean that the laws in force in each Member State are identical. This is because the requirement of transposition does not require that the text of a directive be copied word for word into legislation in the Member State. This is because Member States are afforded some room for maneuver in interpreting and applying the main requirements of a directive in the context of their own respective legal systems.

As a result of this, data protection legislation may often differ in terms of both its form and substance from one Member State to another (though such difference should not in theory be major). Some Member States may for example have transposed the contents of Directive 95/46/EC into one piece of legislation whilst others may have scattered it across several. Some of the directive's requirements may be found in legislation that is specifically related to data protection whilst other may have been inserted into pre-existing pieces of legislation that cover related matters. Given such variation, an exhaustive comparative style review of all of the data protection provisions in the various systems of the EU would be beyond the scope of this deliverable. Annex I of this documents contains translations from 4 data protection laws in four member states of the EU. The intention in presenting such a selection is not to be exhaustive, but to illustrate the different requirements that may exist in one Member State to another. The material found in Annex I does not represent all of the relevant law in the particular Member State Concerned Relating to Data Protection but rather the main elements that were likely to be of relevance to the FORENSOR project.

5.6 The proposed EU Data protection regulation

In November 2010 the European Commission announced its plans to reform the EU data protection framework. The proposal has been issued on 25 January 2012 and consists of two

---

96 Some of the material here is taken from the Deliverable “Report of relevant legal and normative standards and their evolution” from the ADVISE project (Advanced Video Surveillance archives search Engine for security applications). Grant agreement no. 285024

main instruments: one for the General Data Protection Regulation,\textsuperscript{98} meant to replace the 1995 Data Protection Directive, and the Police and Criminal Justice Data Protection Directive,\textsuperscript{99} meant to replace the Framework Decision 2008/977/JHA. The proposed reform is a fruit of some two years of preparations and it opens up a law) making process that is intended to take at least as much time. One of the main aims of the proposal is to provide an adequate response to the contemporary challenges of the information society. The reform proposes considerable changes. According to the Commission’s press release,\textsuperscript{100} the key changes in the data protection reform include:\textsuperscript{101}

A single set of rules on data protection, valid across the EU. It would be a regulation and not a directive, thus once adopted and entered into force, it would be directly applicable in all Member States. This is an important and far reaching development; once finalized, the new instrument is expected to affect the way Europeans work and live together.\textsuperscript{102} In particular it is hoped that the regulation will mean:

\begin{itemize}
\item Unnecessary administrative requirements, such as notification requirement, will be removed.
\item Instead, the Regulation provides for increased responsibility and accountability for those processing personal data. These accountability tools would include data breach notification, appointment of the internal data protection officer and an obligation to conduct a data protection impact assessment.
\item Organisations will only have to deal with a single national data protection authority in the EU Member State where they have their main establishment. Likewise, people can refer to a data protection authority in their country, even when their data is processed by a company based outside the EU.
\item Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed.
\end{itemize}


\textsuperscript{102} P. De Hert and V. Papakonstantinou, (2012).
• People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily (right to data portability).
• The so-called “right to be forgotten” will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.
• EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.
• Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules.
• A new Directive will apply general data protection principles and rules for police and judicial cooperation in criminal matters. The rules will apply to both domestic and cross border transfers of data.

6 Rules and Principles pertaining to the Use of Images and Videos in Criminal Proceedings.

The aim of the FORENSOR project is to develop a prototype that will not only be capable of alerting the police and other authorities to the possible existence of criminal activities and other issues, but also to provide material that could be used as evidence in criminal proceedings. In order to be able to made use of in such a manner the data that is used will have to have been collected, stored, and handled in a manner that is not only consistent with laws that have already been described in this document, but also with rules concerning the gathering and use of evidence in criminal proceedings. Such laws can be placed in a different conceptual category than the ones described already in this report. The laws and principles discussed in sections 3–5 of this document are relevant to the existence and monitoring of surveillance practices. The second is relevant to how such practices can be used to determine guilt in a court of law. In order for FORENSOR to be suitable for its desired use it is thus equally important to consider this second category of laws. Failure to do so will mean that images and videos gathered from the FORENSOR device will not be capable of being used in criminal proceedings. Three types of rules would govern admissibility of digital evidence in criminal proceedings, these are; (i) general rules concerning due process in criminal proceedings; (ii) general rules of evidence in criminal proceedings and; (iii) specific rules relating to digital evidence in criminal proceedings.  

Each of these is considered in the following

103 Further information is available from “The Admissibility of Electronic Evidence in Court: Fighting Against High Tech Crime” created within the context of the the CYBEX initiative concerned with the
sub sections of this document. It will be necessary for those involved in the design of a FORENSOR prototype to be available of these principles so that such a prototype is, to as great an extent as possible, capable of facilitating good practices with regards to the gathering and use of evidence.

6.1 General Rules Concerning Due Process in Criminal Proceedings

Criminal proceedings are not an even affair - the two proponents in such a ‘struggle’ are not equally matched. On the one hand there exists the defendant(s), who are usually private individuals and who only have meagre resources to apply to the proceedings in question (for example the ability to hire an advocate if they can even afford that). On the other exists the state and its criminal justice machinery. Such machinery exists inter alia of the police, the administrative criminal justice system and the prisons. Given this disparity of resources that each party can apply to the proceedings in question there would be little chance of a fair hearing unless rules exist to restrain the state and its machinery and ensure that it operates in a proper way. The purpose of such rules are to ensure that the criminal justice system of the state acts in a proper way, permitting a fair hearing of the facts in the case in order to allow a fair determination of guilt or innocence. Part of acting in a proper way entails only presenting evidence that is real and relates to question that exists before the court. The idea of ‘due process’ is central to this. It ensures that proper procedures exist so as to ensure that evidence is collected, processed and presented in a valid way to the courts. Such rules exist to prevent abuse and the risk of miscarriages of justice. Article 6 of the European Convention on Human Rights (which is binding in most European Legal systems) for example states:

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

---

Admissibility of Electronic Evidence in Court. Available at: https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf


2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

   (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;

   (b) to have adequate time and the facilities for the preparation of his defence;

   (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

   (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

   (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 6 itself does not contain explicit mention of the gathering of evidence. Nor does it describe specific rules that are applicable to the gathering of evidence. The ECtHR has stated that such specific rules are a matter for Member States of the CoE to decide upon for themselves.\(^{106}\) There are however a number of implicit general principles which the ECtHR has recognized apply to the collection and use of evidence in criminal proceedings and may be likely to be relevant to FORENSOR. National rules pertaining to the collection and use of evidence in such matters should be read in the light of such principles.\(^{107}\) These are described below.

6.1.1 Fairness

Above all exists the principle that the evidence in question must have been collected in a fair manner. Crucial aspects in determining fairness are that the evidence must have been collected

---

106 CASE OF SCHENK v. SWITZERLAND (Application no.10862/84)
lawfully and that it has not be done so it a way that has violated any legal rights the defendant may possess (including *inter alia* Human Rights as outlined by the ECHR). This will include individual privacy rights as discussed in section 4. It is important that in “determining whether the proceedings as a whole were fair, regard must also be had to whether the rights of the defence have been respected. In particular, it must be examined whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use.”108

6.1.2 Quality

Article 6 ECHR also has implications in terms of the quality of evidence that is used. In criminal proceedings the quality of the evidence must be examined in addition to the way it was obtained. Tribunals must give consideration to anything that would create doubts as towards reliability or accuracy. This is particularly important where certain evidence represents the primary or sole case being made by the state. Whilst it is possible to make a case on a single source of evidence this is only where its quality is of sufficient standard. Where the quality of the evidence in question is weak, supporting evidence of another kind should also be required.109 For an example of such requirements in the national context see Annex IV of this document which inter alia describes rules related to adequacy of evidence drawn from the Portuguese Constitution.

6.1.3 Issues related to entrapment

The ECtHR has accepted that covert surveillance is a necessary part of police investigation into criminal activity of a serious nature. The use of concealed surveillance itself is not therefore itself (if conducted properly) in violation of the law.110 The rise of organized crime in particular requires that “States to take appropriate measures [to tackle such problems], the right to a fair trial, from which the requirement of the proper administration of justice is to be inferred, nevertheless applies to all types of criminal offence, from the most straightforward to the most complex.”111

---

108 RIGHT TO A FAIR TRIAL - ARTICLE 6 OF THE CONVENTION – CRIMINAL LAW” Council of Europe/European Court of Human Rights, 2014 p 24
109 CASE OF BYKOV v. RUSSIA (Application no. 4378/02), CASE OF JALLOH v. GERMANY (Application no.5481/00)
110 CASE OF RAMANAUSKAS v. LITHUANIA (Application no.74420/01)
111 RIGHT TO A FAIR TRIAL - ARTICLE 6 OF THE CONVENTION – CRIMINAL LAW” Council of Europe/European Court of Human Rights, 2014 p 25
In this context, the Court has stated that the police whilst permitted to act undercover may not act in a way that is itself intended to incite criminal activity.  

6.1.4 Appropriate oversight

Whilst the ECtHR has accepted the possibility of covert surveillance activities, it has stated that given there is a potential to infringe upon individual rights. In order to reduce this risk, such activities should be supervised by suitable individuals or organisations. This may include investigatory judges or in appropriate circumstances prosecutors.

6.2 Common rules and principles pertaining to digital evidence

Digital evidence is of such a nature that it can be thought of as posing extra risks than conventional i.e. non digital evidence. This is for a number of reasons. “Most importantly digital files and documents are easy to manipulate. They can be copied, altered, updated, deleted (which does not mean expunged) or intercepted, leaving the lawyer with the problem of advising the client as to what is reasonable when searching or requesting documents. Metadata is often hidden (the term metadata refers to the ‘data about data’. In digital documents, metadata tends to be information that is not visible on screen.” Given the nature of digital evidence, the risks are higher for all of the traditional threats to occur to the fair management and presentation of evidence, including falsifying, destroying and manipulation of evidence. Furthermore, the complexity of digital evidence means that not only is the risk of falsification greater, but also the risk that criminal proceedings become derailed or halted because of procedural irregularities. This is because the more complex the nature of the evidence, the greater the possibility that such evidence can be challenged on procedural irregularities. It is therefore important in such cases that great attention in given to the the procedural requirements in place in the particular context in question.

112 CASE OF KHUDOBIN v. RUSSIA (Application no. 59696/00)
113 CASE OF BANNIKOVA v. RUSSIA (Application no.18757/06)
It is not possible to speak of a pan European approach towards digital evidence (just as there are no common European rules for evidence in general). There are however a number of points which by virtue of being good practice apply in most jurisdictions.115 These are:

- There is a lack of established protocol for deciding whether to admit digital evidence; however, a few general rules can be drawn. As there seems to be no “clear and precise rules governing the possibility of using [...] technology in criminal proceedings.”116
- “Due process considerations forbid the usage of illegally obtained evidence before and during the trial proceedings”; “courts exclude evidence that has been obtained as a result of the exploitation of other illegally obtained evidence.”117
- In order for evidence to be admissible it must be relevant, without being prejudicial, and reliable.
- Evidence must be direct, not hearsay or indirect. It must relate to a fact, not to an opinion. (It is the court that can draw its own conclusion).
- “Admissibility is very much related to the possibility, or not, of excluding electronic evidence without prior motive.”118
- Digital evidence must be authentic.119 Therefore information should be given to the court as to the manner in which the data was produced, along with the applications used and steps taken to gather such information. This will include processed using meta data.120
- Evidence must be presented to the court in visible and legible form.121
- It is of paramount importance that anyone handling electronic evidence prior to their examination, treat them in such a manner that will give the best opportunity for any recovered data to be admissible in evidence in any later proceedings.122
- The defendant might contest digital evidence at any given time.

116 From a general overview taken from http://ssrn.com/abstract=1922472
118 https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf
Rules on digital evidence in criminal proceedings are described in the Council of Europe’s Convention on Cybercrime (2011).\(^{123}\) The relevant articles i.e 14-21, are shown in Annex II of this Document.

6.3 General Precautionary Principles to be applied to digital evidence.

A further illustrative example of good practice concerning the use of digital evidence has been produced by the Association of Chief Police Offices (ACPO) of England, Wales and Northern Ireland.\(^{124}\) Although not binding (either in the UK or elsewhere) it can be thought of as representing good practice that is likely to increase the likelihood of compliance with whatever local rules on evidence to be used in criminal proceedings might exist. These principles are:

**Principle 1**: The data held on an exhibit must not be changed.

**Principle 2**: Any person accessing the exhibit must be competent to do so and explain the relevance and the implications of their actions.

**Principle 3**: A record of all processes applied to an exhibit should be kept. This record must be repeatable to an independent third party.

**Principle 4**: The person in charge of the investigation has responsibility for ensuring that the law and these principles are adhered to.

6.3.1.1 Rules on electronic evidence often drawn by analogy

The legal environment with regard to digital forms of evidence is varied across Europe. Some states have specific legislation that refers to digital or ‘electronic’ forms of evidence. Other states use general rules on evidence in an analogous manner and apply them to new technological possibilities as they emerge. In this way courts and judges are often willing to embrace new forms of technological evidence even where such forms are not specifically described in legislation. What is important is that such new forms be capable of being gathered, stored and processed according to the same established principles that apply to more familiar forms of evidence.


\(^{124}\) [http://www.bcs.org/content/ConWebDoc/7372](http://www.bcs.org/content/ConWebDoc/7372)
Particular elements in some of the FORENSOR use case scenarios are briefly summarised below.125

Spain: Relevant Legislation - Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, as amended.126

In Spain, the Criminal Procedure Law includes among the modes of evidence the means of reproducing words, sounds and images as well as instruments permitting the filing and knowing or reproducing words, data, figures and mathematical operations carried out for accounting purposes or other ends, relevant to the trial. Furthermore, in the enumeration of the different formats that can be considered a “document” under the Criminal Code any format containing data is included. Finally, in Spain, the Labour Proceedings Law allows the use of any type of evidence, including those mechanical means of reproducing words, images and sounds.

Portugal: Relevant legislation - Código de processo Penal 127

In the case of Portugal, the Criminal Procedural Code defines documentary evidence as any type of declaration, symbol or note presented in written form or by any other technical means in accordance with the criminal laws of the country, thus including the electronic document. The Portuguese Civil Code also defines documentary evidence, encompassing “mechanical or electronic reproductions of documents”. Lastly, in Portugal we found a definition of electronic documents in the Law on electronic documents and signatures which states that it is what has been elaborated through electronic data processing.

Italy: Relevant legislation - Il codice di procedura penale128

In Italy, the Criminal Code has been updated in accordance with European regulations and contains a text defining the electronic document as any computer tool that contains information with evidentiary value or any software indicated for the processing of this information. Furthermore, this country’s Code of Electronic Government includes the precise meaning of an electronic document, electronic authentication and other concepts such as an electronic identity document or the certification of service suppliers. Particularly, in accordance with what is established in the text, an electronic document would be the electronic representation of acts, deeds or data with legal relevance and, on the other hand, the electronic signature is defined as

125 These excerpts are taken from a report entitled “The Admissibility of Electronic Evidence in Court: Fighting Against High Tech Crime” created within the context of the the CYBEX initiative concerned with the Admissibility of Electronic Evidence in Court. Available at: https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf
128 Available at: http://www.polpenuil.it/attachments/048_codice_di_procedura_penale.pdf
data in electronic form united or associated in a logical manner to other electronic data used as a method of authentication.

**Greece; Relevant legislation - The Greek Code of Criminal Procedure (GCCP) is the primary piece of legislation relating to rules of evidence**

Regarding the means of proof, every lawfully acquired evidence is in principle admissible and can be adduced before Court (Arts. 177, 178 GCCP). Investigating authorities and Courts as well have a duty to search for the factual truth (Arts. 177, 351, 357 GCCP) being entitled to initiate any investigating act with respect to any evidence considered necessary to reveal the truth. Procedural law does not entail rules concerning the probative value of the various means of proof and all lawfully acquired evidence is in principle subject to the Court’s free evaluation. Art. 178 GCCP mentions the most common means of proof: indices, inspection of persons, places and objects, expert’s reports, confessions, statements of witnesses and documents.¹²⁹

---

¹²⁹ This information can be found at the Greek Legal Digest Website at http://www.greeklawdigest.gr/topics/judicial-system/item/16-procedure-before-criminal-courts
Bibliography

C. Bennet, In defence of privacy: The concept and the regime', Surveillance and Society, 8,(4) (2011) pp. 485-496


N. Daniels, Justice, health and healthcare', American Journal of Bioethics, 1,(2) (2001) pp. 2-16


S. Gutwirth, 'Privacy and the Information Age', (Rowman and Littlefield, New York, 2002)


7 Annex I – Examples of The Imposition of Data Protection Law in Use Case Member States

7.1 Portugal

7.1.1 Background

The CNPD\textsuperscript{130} – Comissão Nacional de Protecção de Dados – is the Portuguese Data Protection Authority. The CNPD is an independent body, with powers of authority throughout national territory. It is endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law. The CNPD states that it has the following tasks:

- To supervise and monitor compliance with the laws and regulations in the area of personal data protection.
- To issue prior opinion on any legal provisions and on legal instruments in preparation in Community or international institutions relating to the processing of personal data.
- To exercise investigative powers, having access to data undergoing processing.
- To exercise powers of authority, particularly those of ordering the blocking, erasure or destruction of data, or imposing a temporary or permanent ban on the processing of personal data.
- To warn or publicly censure the data controller for failure to comply with legal provisions on data protection.
- To be engaged in legal proceedings, in case of violation of the Data Protection Act.
- To report to the Public Prosecution Office any criminal offences arising out of its functions and to take the necessary and urgent measures to provide evidence.

\textsuperscript{130} Much of the information in this section is taken from the CNPD website available at: https://www.cnpd.pt/english/index_en.htm
7.1.2 Salient Examples

The main legislative provision is the ‘Act on the Protection of Personal Data (transposing into the Portuguese legal system 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).’

Definitions – Article 3

(a) “personal data” shall mean any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether wholly or partly by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(d) “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by laws or regulations, the controller shall be designated in the Act establishing the organisation and functioning or in the statutes of the legal or statutory body competent to process the personal data concerned;

(e) “processor” shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;
(g) “recipient” shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a law shall not be regarded as recipients;

(h) “the data subject’s consent” shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;

(i) “combination of data” shall mean a form of processing which consists of the possibility of correlating data in a filing system with data in a filing system or systems kept by another or other controllers or kept by the same controller for other purposes.

The processing of sensitive data – Article 7

1 – The processing of personal data revealing philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data, shall be prohibited.

2 – The processing of the data referred to in the previous number shall be permitted by a legal provision or by the authorisation of the CNPD when, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller or when the data subject has given his explicit consent for such processing, in both cases with guarantees of non-discrimination and with the security measures provided for in Article 15.

3 – The processing of the data referred to in 1 shall also be permitted when one of the following conditions applies:

(a) when it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;

(b) when it is carried out with the data subject’s consent in the course of its legitimate activities by a foundation, association or non-profit seeking body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

(c) when it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations;
(d) when it is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.

4 – The processing of data relating to health and sex life, including genetic data, shall be permitted if it is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided those data are processed by a health professional bound by professional secrecy or by another person also subject to an equivalent obligation of secrecy and are notified to the CNPD under article 27, and where suitable safeguards are provided.

**Suspicion of illegal activities, criminal and administrative offences – Article 8**

1 – Central registers relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may only be created and kept by public services vested with that specific responsibility by virtue of the law establishing their organisation and functioning, subject to observance of procedural and data protection rules provided for in a legal order, with the prior opinion of the CNPD.

2 – The processing of personal data relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may be authorised by the CNPD, subject to observance of the rules for the protection of data and the security of information, when such processing is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overriding.

3 – The processing of personal data for the purposes of police investigations shall be restricted to the processing necessary to prevent a specific danger or to prosecute a particular offence and to exercise the responsibilities provided for in the respective implementing statutes or another legal provision or in the terms of an international agreement or convention to which Portugal is party.

**Right of access – Article 11**

1 – The data subject has the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense:

(a) Confirmation as to whether or not data relating to him are being processed and information as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;
(b) Communication in an intelligible form of the data undergoing processing and of any available information as to their source;

(c) Knowledge of the logic involved in any automatic processing of data concerning him;

(d) The rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Act, in particular because of the incomplete or inaccurate nature of the data;

(e) Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (d), unless this proves impossible.

2 – In the case of the processing of personal data relating to State security and criminal prevention or investigation, the right of access may be exercised by means of the CNPD or another independent authority in whom the law vests verification of compliance with legislation on the protection of personal data.

3 – In the cases provided for in 6 above the right of access is exercised by means of the CNPD, securing the constitutional rules applicable, in particular those guaranteeing freedom of expression and information, freedom of the press and the professional independence and secrecy of journalists.

4 – In the cases provided for in (2) and (3), if communication of the data might prejudice State security, criminal prevention or investigation and freedom of expression and information or the freedom of the press, the CNPD shall only inform the data subject of the measures taken.

5 – The right of access to information relating to health data, including genetic data, is exercised by means of the doctor chosen by the data subject.

6 – If the data are not used for taking measures or decisions regarding any particular individual, the law may restrict the right of access where there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy, and when the data are used solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

**Security of processing – Article 14**

1 – The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state
of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2 – Where processing is carried out on his behalf the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

3 – The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to in 1 shall also be incumbent on the processor.

4 – Proof of the will to negotiate, the contract or the legal act relating to data protection and the requirements relating to the measures referred to in 1 shall be in writing in a supporting document legally certified as affording proof.

**Transfer of personal data outside the European Union - Article 19**

**Principles**

1 - Without prejudice to the following Article, the transfer to a State which is not a member of the European Union of personal data which are undergoing processing or intended for processing may only take place subject to compliance with this Act and provided the State to which they are transferred ensures an adequate level of protection.

2 – The adequacy of the level of protection of a State which is not a member of the European Union shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the State in question and the professional rules and security measures which are complied with in that country.

3 – It is for the CNPD to decide whether a State which is not a member of the European Union ensures an adequate level of protection.

4 – By means of the Ministry of Foreign Affairs the CNPD shall inform the European Commission of cases where it considers that a State does not ensure an adequate level of protection.

5 – The transfer of personal data identical to those the European Commission has considered do not enjoy adequate protection in the State to which they are to be sent shall be prohibited.
7.2 Greece

7.2.1 Background

The main Greek legislative initiative translating Directive 95/46/EC is “Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data”.

The Hellenic Data Protection Authority was established with Law 2472/97, which incorporates into the Greek law European Directive 95/46/EC. This Directive sets new rules for the protection of personal data in the member states of the European Union. In addition, the Hellenic Data Protection Authority implements Law 3471/2006 with respect to the electronic communications sector which incorporates into the Greek law European Directive 58/2002.

7.2.2 Salient National Law

Law 2472/97, which incorporates into the Greek law European Directive 95/46/EC is the most important legislative initiative.

Key Definitions – Article 2

a) "Personal data" shall mean any information relating to the data subject. Personal data are not considered to be the consolidated data of a statistical nature whence data subjects may no longer be identified.

b) "Sensitive data" shall mean the data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership to a trade-union, health, social welfare and sexual life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas. In particular, in cases of criminal charges or convictions, it is possible to allow their publication by the Public Prosecutor's Office for the offences referred to in item b, paragraph 2 of Article 3 following an order by the competent Public Prosecutor of the Court of First Instance or the chief Public Prosecutor if the case is pending before the Court of Appeal. The publication of criminal charges or convictions aims at the protection of the community, of minors

---

131 This material is taken from the EU Commission’s Website concerning the transposition of directive 95/46/EC available at: http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm
The material here for Greece represents an unofficial translation available at: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-APRIL010-EN%20_2_.PDF
132 Information on the data protection background in Greece is available in Greek and English in the site of the Hellenic Data Protection Authority, available at: http://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL
and of vulnerable or disadvantaged groups, as well as at the facilitation of the punishment of those offences by the State.

c) "Data Subject" shall mean any natural person to whom such data refer and whose identity is known or may be found, i.e., his/her identity may be determined directly or indirectly, in particular by reference to an identity card number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, political or social identity.

d) "Processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data by Public Administration or by a public law entity or private law entity or an association or a natural person, whether or not by automatic means, such as collection, recording, organisation, preservation or storage, modification, retrieval, use, disclosure by transmission, dissemination or otherwise making available, correlation or combination, interconnection, blocking (locking), erasure or destruction.

e) "Personal Data File" ("File") shall mean any structured set of personal data which are accessible on the basis of specific criteria.

f) "Interconnection" shall mean a means of processing consisting in the possibility of co-relating the data from a file to the data from a file or files kept by another Controller or Controllers or with data from a file or files kept by the same Controller for another purpose.

g) "Controller" shall mean any person who determines the scope and means of the processing of personal data, such as any natural or legal person, public authority or agency or any other organisation. Where the purposes and means of processing are determined by national or Community laws or regulations, the Controller or the specific criteria for his/her nomination shall be designated by national or Community law.

h) "Processor" shall mean any person who processes personal data on behalf of a Controller, such as any natural person or legal person, public authority or agency or any other organisation.

i) "Third party" shall mean any natural or legal person, public authority or agency or any other body other than the data subject, the Controller and the persons authorised to process the data, provided that they act under the direct supervision or on behalf of the Controller.

j) "Recipient" shall mean any natural or legal person, public authority or agency or any other organisation to whom data are disclosed or transmitted, whether a third party or not.

k) "The Data Subject's Consent" shall mean any freely given, explicit and specific indication of will, whereby the data subject expressly and fully cognisant signifies his/her informed agreement to
personal data relating to him being processed. Such information shall include at least information as to the purpose of processing, the data or data categories being processed, the recipient or categories of recipients of personal data as well as the name, trade name and address of the Controller and his/her representative, if any. Such consent may be revoked at any time without retroactive effect. 

l) "Authority" shall mean the Authority for the Protection of Personal Data, which is established pursuant to Chapter D of this law.

Conditions required for the lawful processing of data – Article 4

1. Personal data, in order to be lawfully processed, must be:

   a) collected fairly and lawfully for specific, explicit and legitimate purposes and fairly and lawfully processed in view of such purposes.

   b) adequate, relevant and not excessive in relation to the purposes for which they are processed at any given time.

   c) accurate and, where necessary, kept up to date.

   d) kept in a form which permits identification of data subjects for no longer than the period required, according to the Authority, for the purposes for which such data were collected or processed. Once this period of time is lapsed, the Authority may, by means of a reasoned decision, allow the maintenance of personal data for historical, scientific or statistical purposes, provided that it considers that the rights of the data subjects or even third parties are not violated in any given case.

2. It shall be for the Controller to ensure compliance with the provisions of the previous paragraph. Personal data, which have been collected or are being processed in breach of the previous paragraph, shall be destroyed, such destruction being the Controller’s responsibility. The Authority, once such a breach is established, either ex officio or upon submission of a relevant complaint, shall order any such collection or processing ceased and the destruction of the personal data already collected or processed.

A Duty of Notification – Article 6

1. The Controller must notify the Authority in writing about the establishment and operation of a file or the commencement of data processing.
2. In the course of the aforementioned notification, the Controller must necessarily declare the following:

a) his/her name, trade name or distinctive title, as well as his/her address. (The second item is deleted, as it is no longer valid) b) the address where the file or the main hardware supporting the data processing are established.

c) the description of the purpose of the processing of personal data included or about to be included in the file.

d) the category of personal data that are being processed or about to be processed or included or about to be included in the file.

e) the time period during which s/he intends to carry out data processing or preserve the file.

f) the recipients or the categories of recipients to whom such personal data are or may be communicated.

g) any transfer and the purpose of such transfer of personal data to third countries.

h) the basic characteristics of the system and the safety measures taken for the protection of the file or data processing.

(The item was deleted pursuant to paragraph 2 of article 8 of Law 2819/2000, Official Gazette A/84)

4. Any modification of the data referred to in paragraph 2 must be communicated in writing and without any undue delay by the Controller to the Authority.

Conditions Required for Processing – Article 5

1. The Controller must notify the Authority in writing about the establishment and operation of a file or the commencement of data processing.

2. In the course of the aforementioned notification, the Controller must necessarily declare the following:

a) his/her name, trade name or distinctive title, as well as his/her address. (The second item is deleted, as it is no longer valid)

b) the address where the file or the main hardware supporting the data processing are established.

c) the description of the purpose of the processing of personal data included or about to be included in the file.
d) the category of personal data that are being processed or about to be processed or included or about to be included in the file.

e) the time period during which s/he intends to carry out data processing or preserve the file.

f) the recipients or the categories of recipients to whom such personal data are or may be communicated.

g) any transfer and the purpose of such transfer of personal data to third countries.

h) the basic characteristics of the system and the safety measures taken for the protection of the file or data processing.

i) (The item was deleted pursuant to paragraph 2 of article 8 of Law 2819/2000, Official Gazette A/84)

3. The data referred to in the preceding paragraph will be registered with the Files and Data Processing Register kept by the Authority.

4. Any modification of the data referred to in paragraph 2 must be communicated in writing and without any undue delay by the Controller to the Authority.

**Processing of sensitive data – Article 7**

1. The collection and processing of sensitive data is prohibited.

2. Exceptionally, the collection and processing of sensitive data, as well as the establishment and operation of the relevant file, will be permitted by the Authority, when one or more of the following conditions occur:

   a) The data subject has given his/her written consent, unless such consent has been extracted in a manner contrary to the law or bonos mores or if law provides that any consent given may not lift the relevant prohibition.

   b) Processing is necessary to protect the vital interests of the data subject or the interests provided for by the law of a third party, if s/he is physically or legally incapable of giving his/her consent.

   c) Processing relates to data made public by the data subject or is necessary for the recognition, exercise or defence of rights in a court of justice or before a disciplinary body.
d) Processing relates to health matters and is carried out by a health professional subject to the obligation of professional secrecy or relevant codes of conduct, provided that such processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services.

e) Processing is carried out by a Public Authority and is necessary for the purposes of aa) national security, bb) criminal or correctional policy and pertains to the detection of offences, criminal convictions or security measures, cc) protection of public health or dd) the exercise of public control on fiscal or social services.

f) Processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken.

g) Processing concerns data pertaining to public figures, provided that such data are in connection with the holding of public office or the management of third parties' interests, and is carried out solely for journalistic purposes. The Authority may grant a permit only if such processing is absolutely necessary in order to ensure the right to information on matters of public interest, as well as within the framework of literary expression and provided that the right to protection of private and family life is not violated in any way whatsoever.

3. The Authority shall grant a permit for the collection and processing of sensitive data, as well as a permit for the establishment and operation of the relevant file, upon request of the Controller. Should the Authority ascertain that processing of sensitive data is carried out, the notification of the existence of such a file pursuant to article 6 of this law is considered to be a request for a permit. The Authority may impose terms and conditions for a more effective protection of the data subjects’ or third parties’ right to privacy.

4. The permit will be issued for a specific period of time, depending on the purpose of the data processing. It may be renewed upon request of the Controller.

5. The permit shall necessarily contain the following:

   a) The full name or trade name or distinctive title, as well as the address, of the Controller and his/her representative, if any.

   b) The address of the place where the file is established.

   c) The categories of personal data which are allowed to be included in the file.
d) The time period for which the permit is granted.

e) The terms and conditions, if any, imposed by the Authority for the establishment and operation of the file.

f) The obligation to disclose the recipient or recipients as soon as they are identified.

6. A copy of the permit shall be registered with the Permits Register kept by the Authority.

7. Any change in the data referred to in paragraph 5 shall be communicated without undue delay to the Authority. Any change other than a change of address of the Controller or his/her representative shall entail the issuance of a new permit, provided that the terms and conditions stipulated by law are fulfilled.

Duty of Confidentiality and Security – Article 10

1. The processing of personal data shall be confidential. It shall be carried out solely and exclusively by persons acting under the authority of the Controller or the Processor and upon his/her instructions.

2. In order to carry out data processing the Controller must choose persons with corresponding professional qualifications providing sufficient guarantees in respect of technical expertise and personal integrity to ensure such confidentiality.

3. The Controller must implement appropriate organisational and technical measures to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data subject to processing. Without prejudice to other provisions, the Authority shall offer instructions and issue regulations in accordance with article 19 paragraph 1 k involving the level of security of data and of the computer and information infrastructure, the security measures that are required for each category and processing of data as well as the use of technology for the strengthening of privacy.

4. If the data processing is carried out on behalf of the Controller, by a person not dependent upon him, the relevant assignment must necessarily be in writing. Such assignment must necessarily provide that the Processor carries out such data processing only on instructions from the Controller and that all other obligations arising from this article shall mutatis mutandis be borne by him.
A Right of Access – Article 12

1. Everyone is entitled to know whether personal data relating to him are being processed or have been processed. As to this the Controller must answer in writing.

2. The data subject shall be entitled to request and obtain from the Controller, without undue delay and in an intelligible and express manner, the following information:

   a) All the personal data relating to him as well as their source.
   b) The purposes of data processing, the recipient or the categories of recipients.
   c) Any developments as to such processing for the period since s/he was last notified or advised.
   d) The logic involved in the automated data processing.
   e) The correction, deletion or locking of data, the processing of which is not in accordance with the provisions of the present law, especially due to the incomplete or inaccurate nature of data and
   f) The notification to third parties, to whom the data have been announced, of any correction, deletion or locking which is carried out in accordance with case (e), taken that the notification is not impossible or does not demand disproportionate efforts.

3. The right referred to in the preceding paragraph and the rights arising from article 13 are exercised by means of a relevant application to the Controller and the simultaneous payment of an amount of money, the amount of which, the method of payment as well as any other relevant matter will be regulated by a decision of the Authority. This amount will be returned to the applicant if his/her request to rectify or delete data is considered valid by the processor or the Authority, in case of an appeal before it. The Controller must in this case provide the applicant without undue delay, free of charge and in an intelligible form, a copy of the rectified part of the data relating to him.

4. Should the Controller not reply within a period of fifteen (15) days or should his/her answer be unsatisfactory, the data subject shall be entitled to appeal before the Authority. In the event the Controller refuses to satisfy the request of the party concerned, s/he must notify the Authority as to his/her response and inform the party concerned as to his/her right of appeal before it.

5. By virtue of a decision by the Authority, upon application by the Controller, the obligation to inform, pursuant to paragraphs 1 and 2 of the present article, may be lifted in whole or in part, provided that the processing of personal data is carried out on national security grounds or for
the detection of particularly serious crimes. In this case the President of the Authority or his/her substitute carries out all necessary acts and has free access to the files.

6. Data pertaining to health matters will be communicated to the data subject by means of a medical doctor.

**A Right to Object to the Processing of One’s Personal Data – Article 13**

1. The data subject shall be entitled to object at any time to the processing of data relating to him. Such objections shall be addressed in writing to the Controller and must contain a request for a specific action, such as correction, temporary non-use, locking, non-transfer or deletion. The Controller must reply in writing to such objection within an exclusive deadline of fifteen (15) days. His/her response must advise the data subject as to the actions s/he carried out or, alternatively, as to the grounds for not acceding to his/her request. In case the objection is rejected, the relevant response must also be communicated to the Authority.

2. If the Controller does not respond within the specified time limit or his/her reply is unsatisfactory, then the data subject has the right to appeal before the Authority and request that his/her objections are examined. Should the Authority consider that such objections are reasonable and furthermore there is a risk of serious damage being caused to the data subject as a result of the processing, it may order the immediate suspension of the processing until a final decision on the objections is issued.

3. Any person shall be entitled to declare to the Authority that s/he does not wish data relating to him to be submitted to processing in order to promote the sale of goods or long distance services. The Authority shall keep a register for the identification of such persons. The Controllers of the relevant files must consult the said register prior to any processing and delete from their files the persons referred therein.

7.3 Italy

7.3.1 Background

Italy’s consolidated data protection code came into force on 1 January 2004. The Code brings together all the various laws, codes and regulations relating to data protection since 1996. In

---

133 This information is taken from the web site of the Italian Data Protection Authority available at: http://www.garanteprivacy.it/home_en/italian-legislation
particular, it supersedes the Data Protection Act 1996 (no. 675/1996), which had come into effect in May 1997.

There are three key guiding principles behind the code:

1. Simplification
2. Harmonisation
3. Effectiveness

The code is divided into three parts. The first part sets out the general data protection principles that apply to all organisations. Part two of the code provides additional measures that will need to be undertaken by organisations in certain areas, for example, healthcare, telecommunications, banking and finance, or human resources. Part three relates to sanctions and remedies. It is expected that the second part of the code will be developed further through the introduction of sectoral codes of practice.

The Italian Data Protection Authority (Garante per la protezione dei dati personali) is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals' dignity. The DPA was set up in 1997, when the former Data Protection Act came into force. Its tasks are set forth in the law (the Data Protection Code 196/2003, which superseded the Data Protection Act 675/1996). They include the following: supervising compliance with the provisions protecting private life; handling claims, reports and complaints lodged by citizens; banning or blocking processing operations that are liable to cause serious harm to individuals; checking, also on citizens' behalf, into the processing operations performed by police and intelligence services; carrying out on-the-spot inspections to also access databases directly; reporting to judicial authorities on serious infringements; raising public awareness of privacy legislation; fostering the adoption of codes of practice for various industry sectors; granting general authorisations to enable the processing of certain data categories; and participating in Community and international activities, with particular regard to the work of joint supervisory authorities as per the relevant international conventions (Schengen, Europol, Customs Information System).

7.3.2 Salient Examples of National Law\textsuperscript{134}

\textsuperscript{134} The information here is taken from an English translation provided by the Italian National data Protection available at: http://www.garanteprivacy.it/web/guest/home_en/italian-legislation
The main legislative initiative is Date Protection Code – Legislative Decree no. 196/2003. The code applies to all processing within the State and its territories. It will also affect outside organisations that make use of equipment located within Italy, which could include e.g. PCs and other computer-based systems (see Section 5 of the Code). If an organisation outside the EU is processing data on Italian territory, it must appoint a representative in Italy for the application of Italian rules (this will be necessary for notifying with the Garante, if notification is due, and providing data subjects with information notices).

(Data Minimisation Principle) Article 4

1. Information systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively.

Definitions - Article 4

1. For the purposes of this Code,

   a) ‘processing’ shall mean any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank;

   b) ‘personal data’ shall mean any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number;

   c) ‘identification data’ shall mean personal data allowing a data subject to be directly identified;

   d) ‘sensitive data’ shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life;
e) ‘judicial data’ shall mean personal data disclosing the measures referred to in Section 3(1), letters a) to o) and r) to u), of Presidential Decree no. 313 of 14 November 2002 concerning the criminal record office, the register of offence-related administrative sanctions and the relevant current charges, or the status of being either defendant or the subject of investigations pursuant to Sections 60 and 61 of the Criminal Procedure Code;

f) ‘data controller’ shall mean any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters;

g) ‘data processor’ shall mean any natural or legal person, public administration, body, association or other agency that processes personal data on the controller’s behalf;

h) ‘persons in charge of the processing” shall mean the natural persons that have been authorized by the data controller or processor to carry out processing operations;

i) ‘data subject’ shall mean any natural or legal person, body or association that is the subject of the personal data;

l) ‘communication’ shall mean disclosing personal data to one or more identified entities other than the data subject, the data controller’s representative in the State’s territory, the data processor and persons in charge of the processing in any form whatsoever, including by making available or interrogating such data;

m) ‘dissemination’ shall mean disclosing personal data to unidentified entities, in any form whatsoever, including by making available or interrogating such data;

n) ‘anonymous data’ shall mean any data that either in origin or on account of its having been processed cannot be associated with any identified or identifiable data subject;

o) ‘blocking’ shall mean keeping personal data by temporarily suspending any other processing operation;

p) ‘data bank’ shall mean any organised set of personal data, divided into one or more units located in one or more places;

q) ‘Garante’ shall mean the authority referred to in Section 153 as set up under Act no. 675 of 31 December 1996.
Data Subject Rights – Article 7

1. A data subject shall have the right to obtain confirmation as to whether or not personal data concerning him exist, regardless of their being already recorded, and communication of such data in intelligible form.

2. A data subject shall have the right to be informed

   a) of the source of the personal data;

   b) of the purposes and methods of the processing;

   c) of the logic applied to the processing, if the latter is carried out with the help of electronic means;

   d) of the identification data concerning data controller, data processors and the representative designated as per Section 5(2);

   e) of the entities or categories of entity to whom or which the personal data may be communicated and who or which may get to know said data in their capacity as designated representative(s) in the State’s territory, data processor(s) or person(s) in charge of the processing.

3. A data subject shall have the right to obtain

   a) updating, rectification or, where interested therein, integration of the data;

   b) erasure, anonymization or blocking of data that have been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed;

   c) certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected.

4. A data subject shall have the right to object, in whole or in part,

   a) on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection;
b) to the processing of personal data concerning him/her, where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys.

Data Processing Principles – Article 11

1. Personal data undergoing processing shall be:

   a) processed lawfully and fairly;

   b) collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;

   c) accurate and, when necessary, kept up to date;

   d) relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;

   e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

Any personal data that is processed in breach of the relevant provisions concerning the processing of personal data may not be used.

7.4 Spain\textsuperscript{135}

7.4.1 Background

The Spanish Agency of data protection enjoys such, independent body with its own budget and full functional autonomy. The AEPD was created in 1992 and became operational in 1994.\textsuperscript{136} It is responsible for ensuring compliance with legislation on data protection and monitoring their implementation, especially in regard to the rights of information, access, rectification, opposition and cancellation of data (ARCO).

\textsuperscript{135} Information taken from and available at http://uk.pricallaw.com/1-520-8264#a708183

\textsuperscript{136} Much of the information in this section is taken from the site of the AEPD. It has content in a number of languages including in English. Available at: http://www.agpd.es/
Laws relating to data protection in Spain can be found in both general and specific sectorial form. The most important of these are described below.

**General laws**

- The Data Protection Act (Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection (Data Protection Directive). It protects individuals with regard to the processing of personal data and the free movement of data.

- The Regulation developing the Data Protection Act was approved by Royal Decree 1720/2007 of 21 December (Data Protection Regulations).

**Sectoral laws**

There are no sector-specific laws regulating the processing of personal data, but there are regulations that contain specific provisions on personal data processing (for example, Law 26/2006 on insurance and reinsurance intermediation). The most relevant regulations are the:

- Spanish Information Society Services Act (Law 34/2002 on information society services and e-commerce).


In addition, specific legal provisions apply to the processing of:

- Files regulated under the electoral regime legislation.

- Files used exclusively for statistical purposes and protected by legislation on public statistical functions.

- Files for storing data contained in personal classification reports referred to in the armed forces personnel legislation.

- Files derived from the Civil Registry and the Central Registry of Convicts and Fugitives.

- Files from video and audio recordings obtained by law enforcement agencies using video cameras.
7.4.2 Salient Examples of National Law

The most important national provision is The Data Protection Act (Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection (Data Protection Directive). It protects individuals with regard to the processing of personal data and the free movement of data.

Scope - Article 2

1. This Act shall apply to personal data recorded on physical media to make them amenable to treatment, and any type of subsequent use of this data by the public and private sectors. This Organic Law shall govern any processing of personal data:

   a) Files maintained by natural persons in the course of a purely personal or household activity

   b) Files subject to the regulations on protection of classified materials.

   c) Files established for the investigation of terrorism and serious organized crime. However, in such cases the data controller shall previously inform its existence, its general characteristics and purpose of the Data Protection Agency.

2. The system of protection of personal data as set out in this Organic Law shall not apply:

   a) Files regulated by the legislation on the electoral system
   b) Those used solely for statistical purposes, and are covered by state or regional legislation on public statistical function.

   c) Files established for the investigation of terrorism and serious organized crime. However, in such cases the data controller shall previously inform its existence, its general characteristics and purpose of the Data Protection Agency.

3. They are governed by specific provisions, and by any special provisions, if any, of this Organic Act, the following processing of personal data:

---

137 These examples come from Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection. The original text in Spanish is available, together with further information at the site of the Spanish Data Protection Authority. Available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf
a) Files regulated by the legislation on the electoral system.

b) Those used solely for statistical purposes, and are covered by state or regional legislation on public statistical function.

c) Those whose purpose is to store the data contained in the personal staff reports legislation Regime staff of the Armed Forces concerns.

d) Derivatives of Civil Registry and the Central Registry of convicts and rebels.

e) From images and sound recorded by the use of video cameras by the Security Forces in accordance with the legislation on the subject.

**Definitions – Article 3**

a) Personal data: Any information concerning physical persons identified or identifiable.

b) File: any structured set of personal data, in whatever form or method of its creation, storage, organization and access.

c) Data processing: Operations and technical procedures of automated or not, enabling the collection, recording, storage, processing, modification, blocking and cancellation, as well as assignments of data resulting from communications, consultations, interconnections and transfers.

d) Responsible for the data controller. natural or legal person, public or private, or administrative body which determines the purpose, content and use of treatment

e) Affected: the natural person to whom the data undergoing processing in paragraph c) of this article refers to.

f) Dissociation procedure: Any processing of personal data so that the information obtained can not be associated with an identified or identifiable person.

g) Processor: the natural or legal person, public authority, agency or any other body which alone or jointly with others processes personal data on behalf of the controller.

h) Subject's consent: Every manifestation of will, freely given, specific and informed by the data subject consents to the processing of personal data that concerned.

i) Assignment or communication of data: any disclosure of data to a person other than the person concerned.
j) public sources: Those files which can be consulted by any person, unhindered by a limiting provision or without requirement, where appropriate, the payment of a fee. Are considered publicly available sources exclusively the publicity register, telephone directories under the terms provided by the relevant legislation and lists of persons belonging to professional associations containing only data on the name, title, profession, activity, academic degree, address and an indication of their group. They also have the character of publicly available sources, newspapers and official gazettes and the media.

**Principles of Data Protection - Articles 4-12**

1. The personal data can only be collected for treatment and subjected to such treatment, if they are adequate, relevant and not excessive in relation to the scope and specific, explicit and legitimate purposes for which they were obtained.

2. The personal data processed may not be used for purposes incompatible with those for which the data were collected. Further processing of data for historical, statistical or scientific purposes shall not be considered incompatible.

3. The personal data shall be accurate and updated so that they respond truthfully to the current situation of the data.

4. If personal data recorded prove to be inaccurate in whole or in part, or incomplete, they will be canceled and officially replaced by the data corrected or completed, without prejudice to the powers those affected by Article 16.

5. The personal data will be canceled when no longer necessary or relevant to the purpose for which it was collected or recorded. There will be preserved in the form which permits identification of data subjects for longer than is necessary for the purposes based on which were collected or recorded. The procedure by which, exceptionally, served historical, statistical or scientific value in accordance with specific legislation be determined, the full maintenance of certain data is decided.

6. The personal data will be stored so as to allow the exercise of the right of access, unless they are legally canceled.
7. Data collection is prohibited by fraudulent, unfair or illegal

Rights of the Data Subject – Article 5

1. persons to whom personal data are requested must be previously informed explicitly, precisely and unequivocally:

   a) The existence of a file or processing of personal data, the purpose of collecting the data and recipients information.

   b) the obligatory or optional nature of their response to the questions put to them character.

   c) the consequences of obtaining data or the refusal to supply.

   d) the possibility of exercising the access rights, rectification, cancellation and opposition.

   e) the identity and address of the controller or, where applicable, by his representative. When the controller is not established in the territory of the European Union and used in data processing means located on Spanish territory, must, unless such equipment is used for transit purposes, a representative in Spain, without prejudice to any action that may be initiated against the controller himself.

2. When questionnaires or other forms are used for collection they shall appear in the same, in clearly legible form, warnings to in the preceding paragraph.

3. The information referred to in subparagraphs b will not be necessary), c) and d) of paragraph 1 if the content it is clear from the nature of the personal data requested or the circumstances in which they are obtained.

4. When personal data have not been obtained from, it must be informed explicitly, precisely and unequivocally by the controller or his representative, within three months at the time of recording information unless and it had been reported earlier, the content of the treatment, the origin of the data, as well as the provisions of letters of letters a), d) and e) of paragraph 1 of this Article.

5. Shall not apply the provisions of the preceding paragraph when a law expressly provides, when treatment has historical, statistical or scientific purposes, or when the information
proves impossible or would involve disproportionate effort, as determined by the Agency for Data Protection or equivalent regional body, considering the number of subjects, the age of the data and the possible compensatory measures. Nor will govern the provisions of the preceding paragraph when the data come from public sources and are intended for the activity advertising or marketing purposes, in which case each communication sent to the person concerned will be informed of the origin of the data and the identity of the controller and of his rights.

Consent – Article 6

1. The processing of personal data require the unequivocal consent of the affected, unless the law provides otherwise.

2. Consent is not required when personal data are collected for the exercise of the Public administrations within the scope of its powers functions; when referring to the parties to a contract or preliminary contract of a business, employment or administrative relationship and are necessary for its maintenance or fulfillment; when the data processing has the purpose to protect a vital interest of the terms of Article 7 paragraph 6 of this Act, or the data contained in sources accessible to the public and their processing it is necessary for the satisfaction of the legitimate aim pursued by the data controller or by the third party to whom 6. communicate data, provided that the rights and freedoms of the data subject are not violated.

3. The consent referred to in Article may be revoked if there is cause to do so and will not be retroactive.

4. In cases where the consent of the treatment of personal data is not necessary, provided that a law otherwise provides, it can object to their treatment when there are legitimate grounds concerning a specific situation personal. In such a case, the data controller shall exclude the data relating to the treatment affected.

Rules on the Use of Sensitive Data

1. According to the provisions of paragraph 2 of Article 16 of the Constitution, no one may be compelled to testify about his ideology, religion or beliefs. When on these data is necessary to seek the consent below it refers to, He will notify the person concerned about their right not to lend.
2. Only with the express written consent of the affected may be processed the personal data which reveal the ideology, trade union membership, religion and beliefs. Files maintained by political parties, trade unions, churches, denominations or religious communities and associations, foundations and other non-profit whose purpose is political, philosophical, religious or trade union are excluded, as to the data relating to their associates or members, without prejudice to the transfer of such data always require prior consent.

3. The personal data which refer to racial origin, health or sex life may be collected, processed and released when, for reasons of general interest, a law so provides or explicit consent.

4. Are prohibited files created with the sole purpose of storing personal data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin, or sex life.

5. The personal data relating to the commission of criminal or administrative offenses may be included in files of the competent public authorities in the cases provided for in the respective regulations.

6. Notwithstanding the provisions of the preceding paragraphs may be processed the personal data referred to Paragraphs 2 and 3 of this article, when the processing is necessary for the prevention or the medical diagnosis, the provision of care or treatment or the management of health services, provided that the data processing is performed by a health professional subject to professional secrecy or by another person also subject to an equivalent obligation of secrecy. They may also be processed data to the previous paragraph when the processing is necessary to protect the vital interests of the data subject or another person, in the event that the data subject is physically or legally incapable of giving consent.

Data Security – Article 9

1. The data controller and, where applicable, the processor must take the necessary technical and organizational measures to ensure the security of personal data and avoid its alteration, loss or unauthorized access, taking account the state of technology, the nature of the data stored and the risks they are exposed, whether from human action or the physical or natural environment.
2. No personal data in files that do not meet the conditions laid down by rules regarding their integrity and security and treatment centers, premises, equipment, systems and programs. Will be recorded in March. Regulation requirements and conditions to be met by the files and the persons involved in the processing of data in Article 7 of this Law shall be laid down.

**Data Confidentiality – Article 10**

The data and those involved at any stage of the processing of personal data are obliged to maintain confidentiality in respect thereof and the duty to protect them. Obligations continue even after the end of the relations the owner of the file or, where appropriate, with the responsible.
Annex II – Relevant Provisions of the Council of Europe’s Convention on Cybercrime

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

   a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;
   b) other criminal offences committed by means of a computer system; and
   c) the collection of evidence in electronic form of a criminal offence.

3. a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

   b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
      (i) is being operated for the benefit of a closed group of users, and
      (ii) does not employ public communications networks and is not connected with another computer system, whether public or private,

   that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable
international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 16 – Expedited preservation of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

   a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

   b) ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to
enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

   a) collect or record through the application of technical means on the territory of that Party, and
   b) compel a service provider, within its existing technical capability:
      (i) to collect or record through the application of technical means on the territory of that Party; or
      (ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
9 Annex III – An Abstract of the Local Data Protection Laws in Chiusi Village

**Article 12 - Collection procedures and requirements on personal data**

1. Personal data processed are:

   a) processed lawfully and fairly;

   b) collected and recorded for security purposes and made usable in other processing operations if those operations are compatible with those purposes;

   c) collected properly, complete and not redundant in relation to the purposes for which they were collected or subsequently processed;

   d) kept for no longer than is absolutely necessary to the fulfillment of institutional purposes of the system, for which they were collected and subsequently processed and, in any case equal to the period of time established by paragraph 3;

   e) treated, with reference to the purpose of monitoring traffic, referred to in article 3, paragraph 6 letter. d) anyway always safeguarding anonymity, after the collection stage, given that, recorded images may contain personal data;

2. Personal data are taken through the installation of surveillance cameras installed throughout the municipality;

3. Cameras referred in paragraph 2 allow, technically, color video shooting under conditions of adequate natural or artificial light otherwise white/black;

4. The data controller will allow filming and capturing detailed physical features of people only if they are functional to the institutional aims of the system activated;

5. Video signals from the camera unit will be posted at the police headquarters in a storage room where the images will be displayed on the monitor and recorded on special servers;

6. Use of video recording system is needed to reconstruct the event according to the purposes provided in this Regulation;

7. Images videotaped captured for urban safety purposes are maintained at the server placed into the local police headquarters, for a period not exceeding seven days following the disclosure,
pursuant to Article 6 paragraph 8 DL n. 11/2009, unless you have to adhere to a specific request by judicial or investigative police and subject to special requirements for further storage;

8. without the case of the request of the judicial investigation and the judicial police in all other cases if needed further storage of data and images recorded, stretching of retention period is subject to a prior checking application from the Authority for the Protection of Personal Data pursuant to Order 8 April 2010. Images stored on the server will be automatically deleted once the period of legal preservation through overdub;

9. In case of processing data after the recording, the exercise of the rights referred in article 15 of these Regulations is guaranteed;

10. access to the information recorded may be used solely by the Manager in charge of the Municipal Police Force for the declared purposes and in the ways stated by Legislative Decree no. 196/2003, this Regulation and by instructions, regulations and security measures established by the Owner or the Manager;

11. data processing made by the video surveillance system does not apply to sensitive data in art.4 paragraph 1 letter. d) D.Lgs.196 / 2003;

12. If for the declared purposes, there is a need to proceed in processing of sensitive data, the same will comply with the requirements of art.20 and Article 22 paragraphs 3 and 9 DLgs.193 / 2006.

Article 13 - Areas subject to surveillance

Use of video surveillance cameras should be only for control of what takes place in public places and areas and it is not allowed in areas of private property.

Article 14 – Using cameras

1. Video surveillance system provides a static shot of the area and does not collect data biometrics or images associated with the recognition of people through crossing or comparison with other specific personal data or with a certain sampling of subjects;

2. for purposes of monitoring the traffic and help in reconstruction of dynamics of a road accident, cameras are set in order to seize a panoramic image of places and people, avoiding overly detailed shots that could violate the privacy of individuals;

3. video surveillance system is unable to automatically detect illicit behaviors nor to report them;
4. mobile cameras can be used, subject to compliance with the provisions of this Regulation:

a) in cases of logistic support to operations conducted by the staff of Municipal Police on site;

b) in case there is a need to focus on controlling specific areas not covered by the video surveillance system in which events occur in urban security or where there is misconduct related to transfer or creation of waste dumps;

c) to control and register illegal acts committed within the scope of the initial registration of the camera and which might get out of control because involved people walked away;

d) in case you need to immediately verify situations of abuse or danger in case of verbal or telephone communication even in areas not covered by the system of video footage.

**Article 15 - Information provided at the time of collection**

1. City of Chiusi, complying with article 13 of Legislative Decree 06/30/2003 n. 196, is obliged to permanently put appropriate road signs up in streets and squares where cameras are positioned, on those signs there should be the following statement: "Police Station - City of Chiusi - Area under video surveillance. Images kept at the Municipal Police of Chiusi" provided with the camera symbol that complies with the disclosure approved by the ruling of Personal Data Protection Act, 8 April 2010.

2. 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.

3. City of Chiusi is obliged to inform local community: about the start of the processing of personal data, about the activation of video surveillance, about any increase in size of the video setup and on any subsequent ending for any cause of data processing performed, in accordance with article 15, with an advance of 10 days, by publishing appropriate posters and / or other means of local diffusion.

4. Detailed rules for placement of signs will conform to those indicated by Data Protection Supervisor with the document of 8 April 2010. Personal data processing for prevention purposes, detection and crime suppression and for urban security purposes could not be provided in accordance with Legislative Decree article 53, in cases where specific reasons of investigation and public safety shall be without prejudice, if information does not allow undertaking of specific functions pursued.
5. Without the cases specifically mentioned in paragraph 4 of this Article 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.

• SECTION II RIGHTS ON DATA PROCESSING

Article 16 - Rights of a person on his data

1. Related to the processing of personal data a person, upon presentation of appropriate request, is entitled:

   a) to obtain confirmation of the existence of processing of data concerning him;

   b) to be informed about the identity of the owner and manager as well as the purposes and methods of processing his data;

   c) to obtain from the controller, without delay and no later than 15 days from the date of receipt of the request, or 30 days after informing him if operations required for a full response are particularly complex or if there are other valid reasons;

2. the right of confirmation of existence of personal data concerning a certain person, even if not yet recorded and intelligible, communication on such data and their origin, as well as the logic applied in case of their processing with electronic tools, methods and purposes on which the treatment is based; the request can not be made by the same person except after at least ninety days from the previous instance, subject to justified reasons;

3. the right of cancellation, anonymization or blocking of data processed unlawfully, including data that need not to be kept for the purposes for which the data were collected or subsequently processed;

4. the right to object, in whole or in part, for legitimate reasons, to the processing of personal data, even if suitable for collection purposes;

5. for each of the requests referred to in paragraph 1, lett. c) n. 1), if not confirmed the existence of data concerning a certain person, by law it may be charged a fee not exceeding the costs actually incurred included the cost of the staff;
6. the rights referred to in this article concerning deceased persons’ personal data may be exercised by whom has a legitimate interest or who acts on behalf of the person involved or for family reasons deserving protection;

7. In exercising the rights stated in paragraph 1 a person may grant, with a written authorization, individuals, institutions, associations or bodies and he may also be assisted by a person of trust;

8. in the event of a negative outcome to the panel referred to the preceding paragraphs, the interested party may apply to the Authority for the Protection of Personal Data, given the possibility of administrative and judicial protection stated by law.

**Article 17 – End of data processing**

In the event of ending, for any reason, of personal data processing they are: a) destroyed; b) kept only for institutional purposes for video setups already started.

- **SECTION III COMMUNICATION AND DIFFUSION OF DATA**

**Article 19 - Communication**

1. The communication of personal data by the municipality of Chiusi for public entities, excluding government-owned entities, is allowed when law or regulation states it. Without such standard, communication it is allowed when it is still necessary and only for the performance of official duties and can be started only if the term in art. 19 paragraph 2 of the Decree. 06/30/2003 n. 196 is extinguished.

2. It is not considered communication, for purposes of preceding paragraph, the knowledge of personal information by people responsible and authorized to perform the processing operations by owner or manager and operating under their direct authority.

3. In any case communication or diffusion of data is required, in accordance with law, police, judicial authorities, information and security agencies or other public pursuant to article 58, paragraph 2, of Legislative Decree. 06/30/2003 n. 196, for defense purposes or state security or prevention, detection or crime suppression.
Annex IV - Principles in Portuguese Law Relating to Criminal Evidence and the Concept of Proportionality

**Principle of adequacy**

The principle of legality and adequacy is reflected in all legislating and principles of law in Portugal. Constitution article 265-A prescribes the Principle of Formal adequacy as follows:

- When the procedure provided, by law, does not suit the specificities, the judge of its own initiative, after hearing the parties, determine the practice of acts that best fit the end of the process, as well as the necessary adjustments.

This wording resulting from DL (Decreto Lei or Bill of Law) 180/96, replaced the DL 329-A / 95 of 12 December, further specifies this principle:

1. When the procedure provided by law does not suit the requirements, the judge must, on its own initiative and with the agreement of the parties, adapt the procedure;
2. During the implementation of the solution referred in the preceding paragraph, the judge determines the course of action that best suited to establishing the truth and correct decision, regardless of which prove to be manifestly defaulter to the end of the process;

Here is stated what was foreseen but wasn't created, only became apparent in Regime Experimental Civil Procedure (Decree No. 108/2006 of 08 June), whose preamble stands out in this regard, the following:

- From a procedural management point is now established, from the judge point of view, the imperatives to adopt the appropriate procedure to the specifics of the case, the content and form from the acts after they in order to achieve and ensure that they are not useless acts, and yet, to make use of procedural streamlining mechanisms established by law.

**Principle of Proportionality**

The principle of proportionality commits the administration an obligation to adjust their actions to the specific purposes that aim to achieve, adjusting the limitations imposed on the rights and interests of other entities, the necessary and reasonable; it is thus a principle that embodies the idea of excess limitation, so that the exercise of powers, namely discretionary, do not exceed the essential for the realization of public goals.

The principle of proportionality is composed of three essential components:

- The adequacy establishing the connection between the means, measures, purposes and objectives;
- The need which translates into the option for less serious action for the interests of individuals and less damaging to their rights and interests;
- The balance, or proportionality in the strict sense, establishes the reporting between the action and the result.

**The Portuguese Constitution, Article 18**

The laws that only restrict rights, freedoms and guarantees, in cases expressly provided in the Constitution, shall be limited to what is necessary to safeguard other constitutionally protected
The organs and administrative agents are subordinated to the Constitution and the law and must act in the exercise of their duties with respect for the principles of equality, proportionality, fairness, impartiality and good faith.

Code of Administrative Procedure, Article 5

The Directors decisions that conflict with subjective rights or legally protected interests of individuals may only affect such positions in terms adequate and proportionate to the objectives to accomplish.

The Portuguese Constitution, Article 32

Are void all evidence obtained through torture, coercion, physical integrity or moral threat to the subject, wrongful interference with privacy, home, correspondence or telecommunications.

Code of Criminal Prosecution, Article 167 (Decree No. 78/87 of 17 February);

Probative value of mechanical reproductions
The photographic, film, phonographic or through electronic process reproductions and, in general, any mechanical reproductions are valid only as evidence, facts or things played if not illegal obtained under criminal law.

Criminal Code, Article 199 - illegal recordings and photographs
1. Who, without consent:
a) Write the words spoken by someone else and not for the public, even if it may be addressed; or
b) Use or allow them to use the recordings referred in the previous paragraph, even if lawfully produced;
It shall be punished with imprisonment up to one year or a fine of up to 240 days.
2. The same penalty who, against their will:
c) a) Taking pictures or filming someone else, even in events that have legitimately participated; or
   d) b) Use or allow them to use photographs or films referred in the previous paragraph, even if lawfully obtained.
3. Is correspondingly applicable the provisions of Articles 197 and 198.