DELIVERABLE REPORT

DELIVERABLE N^0:	D4.1
DISSEMINATION LEVEL:	PUBLIC
TITLE:	EUROPEAN REFERENCE STANDARDS PRIVACY AND DATA PROTECTION
DATE:	17-10-2014
VERSION:	FINAL
AUTHOR(S):	ANTONIO SILVA (INCODE)
REVIEWED BY:	WP LEADER – ESRA BEKTAS (TNO)
APPROVED BY:	COORDINATOR – ANS VAN DOORMAAL (TNO)

GRANT AGREEMENT NUMBER:	312632
PROJECT TYPE:	FP7-SEC-2012.2.1-1 RESILIENCE OF LARGE SCALE URBAN BUILT INFRASTRUCTURE – CAPABILITY PROJECT
PROJECT ACRONYM:	ELASSTIC
PROJECT TITLE:	ENHANCED LARGE SCALE ARCHITECTURE WITH SAFETY AND SECURITY TECHNOLOGIES AND SPECIAL INFORMATION CAPABILITIES
PROJECT START DATE:	01/05/2013
PROJECT WEBSITE:	WWW.ELASSTIC.EU
TECHNICAL COORDINATION	TNO (NL) (WWW.TNO.NL)
PROJECT MANAGEMENT	UNIRESEARCH (NL) (WWW.UNIRESEARCH.NL)

ELASSTIC

Executive Summary

Our starting point is the concept of the ELASSTIC project, a concept for designing safe, secure and resilient large scale building complexes. SMART EVACUATION is the relevant feature in this concept regarding the use of personal data.

This deliverable provides an introduction into the legislation of the EU as well as in more relevant regulation of the member states regarding the handling of personal data.

We analyze the condition of Human Right, Directive 95/46/EC and its protection, also covered by different legislation.

We define the concept of personal data, and the various agents involved as well as the principles to be respected by the processing of personal data.

Contents

1 INTRODUCTION

ELASSTIC is the acronym for Enhanced Large scale Architecture with Safety and Security Technologies and special Information Capabilities. The ELASSTIC project´s objective is to improve the safety, security and resilience of large scale multifunctional building complexes to natural and man-made disasters by providing a methodology and tools which enable to include security and resilience from the early design and planning phase of such projects.

One of the objectives of this project is the development of a blue print of a Smart Evacuation System based on scenarios hazard. This Smart Evacuation will put special attention to building users and because of this, one aspect that will have relevance during the project will be handling personal data that could be used in both the project itself as well as the solutions that may result in accordance with legality.

This procedure must satisfy legal and ethical guidelines and legislation on privacy and data collection related to occupant registration and tracking.

In this deliverable we will analyze what is meant by data protection, the scope of the concept, and also the laws of the EU and the states, identifying the laws of a large sample of states. These are

Spain, Germany, Austria, Belgium, Denmark, France, Greece, Netherlands, Ireland ,Italy, Portugal, United Kingdom ,Sweden and Norway

In this document we have gathered and analyzed relevant rights and laws regarding personal data. We distinguish three categories:

1. The human rights to protection of data. In Chapter 2 and as the starting point we study data protection as a fundamental right enshrined in the Treaty of European Union, the European Convention on Human Rights and its influence as an Universal Human Right in the constitutions of the member states of the EU
2. Data protection regulation in Europe.. In Chapter 3 European legislation is analized: Convention 108, Directive 95/46/EC
3. Protection of data in European comparative law. In Chapter 4 are identified applicable laws of a large sample of states.

Chapter 5 provides the nonjuridical reader with some help by means of explanations, definitions and practical advices. Chapter 6 finally summarizes the main observations and points of attention for the ELASSTIC project to consider.

2 FUNDAMENTAL RIGHTS LIABLE TO BE AFFECTED BY PROTECTION OF DATA

First at all we must to be clear about that personal data are Fundamental Rights, a very important part of the Human Rights

The right to protection of personal data is defined by the European Data Protection Supervisor as “a fundamental right. It is different from, but closely linked to, the right to respect for private and family life. This distinction is notably made in the EU Charter of Fundamental Rights - which mentions the two rights separately, although next to each other in Articles 7 and 8.

Data protection is highly developed in the EU. The central piece of legislation is Directive 95/46/EC, which regulates the protection of individuals with regard to the processing of personal data and the free movement of such data. Implemented into national laws, the Directive applies to all EU Member States as well as to Iceland, Liechtenstein and Norway.

Regulation (EC) No 45/2001 lays down the same rights and obligations, but on the level of the EU institutions and bodies. It also establishes the European Data Protection Supervisor as independent supervisory authority with the task of ensuring that the Regulation is complied with.

Citizens who feel that their rights have been infringed should contact the competent data protection authority, at national or European level

2.1 HUMAN RIGHTS IN THE EUROPEAN UNION

According to the European Union Treaty, the EU is based on the values of human dignity, liberty, democracy, equality, the rule of law and respect for human rights.

The EU recognizes the rights, liberties and principles set out in the Charter of Fundamental Rights of the European Union, of December 7, 2000, in the form in which it was adopted on December 12, 2007 in Strasbourg. The Charter has the same legal value as the treaties.

The fundamental rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and those arising from constitutional traditions common to the member States form, as general principles, part of EU Law.

Conscious of its spiritual and moral heritage, the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity; it is based on the principles of democracy and the rule of law. It places the individual at the heart of its activities, by the institution of Union citizenship and by creation an area of freedom, security and justice.

(…)

To this end it is necessary to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter.

In light of these technological advances, the rights which ought to be fundamentally protected are those relative to the protection of private life as these are the ultimate expression of the right to personal privacy.

2.2 THE RIGHT TO PERSONAL PRIVACY DISCUSSION AND CONCLUSION

In Europe

The Universal Declaration of Human Rights was adopted by the General Assembly of the United Nations on December 10, 1948. According to Article 12:

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.

The International Covenant on Civil and Political Rights was adopted and made available to be signed, ratified and adhered to by the United Nations General Assembly on December 16, 1966. Article 17 states:

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.*

With very similar wording and content, both international texts unequivocally guarantee the protection of private life.

Similarly, the European Convention on Human Rights guarantees *the right to respect for one's private life*. According to Article 8:

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

However, no additional references are to be found concerning the reach or the scope of the protection of the right to respect for private life. As far as this respect is concerned, the conceptions expressed by the legislation of the member States should be those taken into consideration.[1]

Finally, according to Article 7 of the Charter of Fundamental Rights of the European Union:

Everyone has the right to respect for his or her private and family life, home and communications.

The European Court of Human Rights has itself affirmed on numerous occasions that *private life is a broad term not susceptible to exhaustive definition*. This state of affairs, together with a progressive interpretation of the Convention, makes it possible for new powers, derived from the notion of a "private life", to be recognized whenever the conditions of life in a society make it necessary. The precept has enormous potential given the growing technological capacity for social control possessed by modern states.[2]

[1] XABIER ARZOZ SANTIESTEBAN, *"Videovigilancia, Seguridad Ciudadana y Derechos Fundamentales",* Ed. Aranzadi, 2010.

[2] XABIER ARZOZ SANTIESTEBAN, *"Videovigilancia, Seguridad Ciudadana y Derechos Fundamentales",* Ed. Aranzadi, 2010.

The European Court of Human Rights has reiterated that the Convention *is a living instrument that (…) must be interpreted in the light of present-day conditions and it is designed to safeguard the individual in a real and practical way as regards those areas with which it deals*.[3]

The Court has stated in this regard that *increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data.*[4]

For the purposes of the Convention the distinction between private and public life does not coincide with the distinction between private and public space. Together with those factors that we can consider more or less *internal and static* (although not immutable) that affect the individual and the most intimate areas of their life, the standard notion of private life also includes distinctly *external and dynamic* aspects in relation to other individuals. In agreement with the model most often endorsed by the Court, and which most closely constitutes a legal definition of the content of the law, Article 8 of the European Convention on Human Rights protects *a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and may include activities of a professional or commercial nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".*[5]

Thus the concept of private life consists of two dimensions: *spatial and material*.

Spatial Dimension: According to the jurisprudence of the ECHR, there is no doubt that the scope of private life is not restricted to the private or domestic. Scientific doctrine has already made clear which publicly conducted activities and which public places fall under the protection of Article 8 of the ECHR. For the Court, the reasonable expectations of the individual themselves were to be taken into account when deciding if an aspect of their private life is protected against unlawful intrusions.

Material Dimension: This idea protects the right to personal development and a right to establish and develop relationships with other people and with the outside world. From the jurisprudence relevant to the scope of the protection provided by Article 8.1 comes the underlying concept: the notion of personality. The supervisory bodies of the ECHR have established a doctrine that goes beyond the literal definition of the expression "private life" in order to include a wide range of principles and of expressions of individual personality.

Due to the enormous ramifications of this concept the European Commission of Human Rights has frequently invoked the concept of personality in the context of Article 8.1 of the ECHR. The Court also views Article 8 as *a right to free expression and development of an individual's personality*, as *a right to personal development*, as a guarantee *primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings* and highlights that *the idea of personal autonomy is an important principle which underlies the interpretation of its guarantees*.[6]

---

[3] *Airey v. Ireland*, Judgment of October 9, 1979, no. 6289/73, par. 26, ECHR; *Cossey v. United Kingdom*, Judgment of September 27, 1990, no. 10843/84, par. 35 and 42, ECHR; *Stés Colas Est and others v. France,* Judgment of April 16, 2002, no. 37971/97, par. 41, ECHR

[4] *Vonn Hannover v. Germany*, Judgment of June 24, 2004, no. 59320/00, par. 70, ECHR

[5] Refer to, among others, *Bensaid v. The United Kingdom,* Judgment of February 6, 2001, no. 44599/98, par. 47, ECHR; *Peck v. The United Kingdom,* Judgment of January 28, 2003, no. 44647/98, par. 57, ECHR

[6] Refer to, among others, *Fretté v. France*, Judgment of January 30, 2002, no. 36515/97, par. 32, ECHR; *Bensaid v. The United Kingdom,* Judgment of February 6, 2001, no. 44599/98, par. 47, ECHR; *Peck v. The United Kingdom,* Judgment of January 28, 2003, no. 44647/98, par. 57, ECHR; *Botta v. Italy*, Judgment of February 24, 1998, no.

In light of ECHR case law, the enormous potential of the concept of private life is undeniable as it increasingly encompasses aspects of the development of individual personality and penetrates into every area of the law (procedural, criminal, family, immigration, environmental, data protection, access to administrative information, etc.) Doubtless the rights expressly set out by the Convention limit the right to respect of private life, but there is no such obstacle preventing Article 8 from becoming a subsidiary protection in exceptional cases. The difference, with respect to a general freedom to act, would be that those cases would have to be relevant to the notion of private life endorsed by the ECHR in order for Art. 8 to provide effective protection.[7]

It is not possible to abstractly determine which measures affect private life. The question must always be tackled according to the circumstances of the case at hand. However, the following general guidelines can serve as a preliminary abstract limit for the scope of the protection available:

1. The activity in question must have sufficient substance and must be capable of being considered an expression of personality.
2. The consequences of the measure in question must be sufficiently serious.
3. The right to respect of private life can be restricted when *the individual allows their private life to come in contact with public life or in close proximity to other protected interests (i.e. the private life of other individuals)*.

This notion of private life embraces the wide range of available investigative and surveillance techniques and procedures used by authorities.

In effect, as subsequent case law makes apparent, regardless of the device or technology employed, private life is affected when material gathered is processed and personal data is collected for the purpose of identification of an individual with the help, in turn, of additional personal data.

If the premise is accepted that social interaction in public places is characterized by common and reciprocal visibility, the presence of an "electronic eye" modifies the legal definition of observation because the eye does not just see but also systematically and constantly records images.

The European Court of Human Rights confirms, in the *Peck* decision, this interpretation:

The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life (see, for example, Herbecq and Another v. Belgium, applications nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, DR 92-A.P.92). On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations.

The fundamental difference between electronic surveillance and video surveillance lies in the enormous possibilities brought into play by the use of the technology incorporated into the latter: technical possibilities which the human eye and brain lack. Recorded images can be stored indefinitely and processed and used for various purposes without the knowledge of the data subjects. Life in a society can imply a certain level of reciprocal visibility but the possibility of a permanent or systematic register of activities carried out in public represents a quantum leap. This quantum leap disrupts the protection intended in Article 8 of the ECHR.[8]

As the ECHR made clear in the *Perry* case:

[7] XABIER ARZOZ SANTIESTEBAN, *"Videovigilancia, Seguridad Ciudadana y Derechos Fundamentales",* Ed. Aranzadi, 2010.

[8] *Hannover v. Germany*, Judgment of June 24, 2004, no. 59320/00, par. 70, ECHR

The permanent recording of the footage and its inclusion in a montage for further use may therefore be regarded as the processing or collecting of personal data about the applicant.

In effect, if anything should be highlighted from this new decision it should be, precisely, the emphasis given to the existence of processing or use of personal data.

2.2.1 EXTENT OF THE PROTECTION OFFERED BY THE RIGHT TO PRIVACY IN COMPARATIVE LAW

As we've seen, the scope of protection of the right to respect of private life provided by the European Convention on Human Rights must be interpreted in relation to the conceptions expressed in the national legislations of the Member States.

The constitutional evolution of this right varies widely depending on the legal systems of different countries in Europe. There are legal systems in which privacy is fully recognized at the constitutional level (i.e. Belgium, Holland and Spain), others which only include declarations of the right to privacy (Germany and Italy) and, lastly, legal systems which neither include the right nor declarations to its effect in their constitutions (France) but instead recognize the right to privacy in legislation.

Spain

According to Article 18.1 of the Spanish Constitution of 1978:

The right to honor, personal and family privacy and one's own likeness is guaranteed.

According to the Spanish Constitutional Court, Article 18.1 EC, "*implies the defence and guarantee of the private domain of the individual*."[9] According to STC 110/1984, "the explicit recognition in a constitutional text of the right to privacy is very recent and is found in very few constitutions, the Spanish Constitution being one of them. However, its foundation, respect for private life, already appears in some traditional freedoms. (…). This has occurred because modern technology and the evolution of mass media has forced protection to be extended beyond the simple securing of the home as a physical space in which privacy and respect for correspondence prevail. The home is now a place where aspects of private life can be observed. This explains the global recognition of the right to privacy or to private life which excludes interference by any means in those areas reserved for living.

The right to privacy implies *the existence of a proprietary reserved domain in which individuals are protected from interference and surveillance by others. This is necessary, in accordance with the foundations of our culture, in order to maintain a minimum quality of life*.[10]

The concept of privacy has been identified with the following expressions: *private domain of the individual*[11]; *domain reserved for living*[12]; *spatial or functional domain of an individual intended to safeguard privacy and which must remain immune to external aggression from other individuals or from Public Administration*[13]*; proprietary and reserved domain in where individuals are protected from the*

[9] STC 22/1984, FJ 2

[10] SSTC 231/1988, FJ 3 and 57/1994, FJ 5

[11] STC 22/1984, FJ2

[12] STC 110/1984, FJ 3

[13] ATC 642/1986, FJ 3

actions and eyes of others[14]*; a domain an individual reserves for themselves according to the most basic elements of an individual's self-determination*[15]

In reality, a broad definition of privacy is evolving and as such the right to personal privacy is not confined to domestic or private domains but also extends to public domains.

Initially, Spanish constitutional case law identified privacy with a *proprietary and reserved domain in which individuals are protected from the actions and eyes of others. This is necessary, in accordance with the foundations of our culture, in order to maintain a minimum quality of life."*[16]

The right was intended to protect against intrusions, by whatever means they were carried out, into domains reserved for living[17]. However, the reiterated concept of a "reserved domain" was ineffective because it suggested a special understanding of the protected domain.

STC 119/2001 affirmed, for the first time, that the right to privacy, as the fundamental right to physical and moral integrity, and the inviolability of the home are:

Rights which have also taken on a positive dimension with relation to the free development of the personality (…) In effect, given that our constitutional text does not enshrine purely theoretical or illusory laws, but rather those that are real and effective (STC 12/1994 January 17, FJ 6) it is essential that their protection be insured (…) also against those risks which can arise in a technologically advanced society (FJ 5)

Subsequently, in the same judgment it is reiterated that *the object of the right to personal and family privacy (Art. 18.1 EC) refers to an area of an individual's life excluded from the knowledge of others and from intrusions by third parties. The limits of that area must permit the free development of personality.*

Summing up, the clause covering the free development of personality seems to have converted itself into not only the criterion by which the content of the rights granted by Art. 18 EC is interpreted but also into the decisive standard by which it is determined if fundamental rights are being interfered with.

One manifestation of the right to personal privacy which has taken on a life of its own is the right to one's own likeness. The right to privacy and the right to one's own likeness constitute, along with the right to respect of honor, personality rights. Constitutional case law has also expressly highlighted the common objective of both rights:

- *The rights to personal privacy and to one's own likeness, guaranteed by Art. 18.1 of the Constitution, form part of the asset of personality which is included in the scope of private life. These rights safeguard a domain of personal and family privacy which remains sheltered from the intrusions of others. In this domain, faced with the increasing development of means and procedures for the capture, dissemination and broadcast of private images and personal data and circumstances , the necessary protection of the right to one's own likeness, guaranteed by this precept, takes on singular importance."*[18]
- *The right to one's own image, enshrined along with the rights to personal and family privacy and to honor by Art. 18.1 EC, contributes to the preservation of an individual's personal dignity (Art. 10.1 CE) and safeguards a reserved personal sphere protected from illegitimate intrusions by third parties. Physical appearance (…) constitutes the most important defining characteristic of an individual's privacy and of their personal sphere, being a basic means of identification and of*

[14] SSTC 231/1988M, FJ 3 and 57/1994, FJ 5

[15] STC 143/1994, FJ 5

[16] SSTC 231/1988 and 57/1994

[17] STC 119/1984

[18] STC 170/1987, FJ 4

exterior projection, and is an essential factor in an individual's self-recognition. In this context, the capture and broadcast of the likeness of an individual will only be permissible when that individual's own –and previous- conduct or the circumstances in which the individual finds themselves justify the relaxing of restrictions such that conflicting third party or public interests might prevail."[19]

The constitutional affirmation of the right to one's own likeness permits the protection afforded to the right to continue being related to, but not fully coincide with, the scope of protection of personal and family privacy. This conception also underlies Organic Law 1/1982 which provides protection for one's own likeness separate from that enjoyed by personal privacy or private life. According to Art. 7.5 of this law *the capture, reproduction or publication, on film, or by any other means, of an individual's likeness, inside or outside of the context of any part of their private life, except in situations laid out in Art. 8.2,* is considered an illegitimate intrusion.

In the same manner, STC 81/2001 expressly affirms the autonomous character of the right to one's own likeness in the Spanish Constitution. According to the Constitutional Court *it should not be ignored that the capture and publication of an individual's likeness can infringe both upon their right to honor and to privacy. However,* ***the specific character of the right to one's own likeness implies protection against the reproduction of an individual's likeness which, while affecting the personal sphere of the owner, does not damage their good name or reveal aspects of their private life.***[20]

In its constitutional dimension, the right to one's own likeness, enshrined in Art. 18.1 EC, is a personality right derived from human dignity and intended to protect an individual's moral dimension. Both of which confer upon the owner a right to determine what graphical information originating from their physical features can be publicly broadcast. The authority granted by this fundamental right essentially prohibits the collection, reproduction or publication of an individual's likeness by unauthorized third parties -whatever the objective: informational, commercial, scientific, cultural, etc.

In the Spanish constitution, the right to one's own likeness is an autonomous right even though, as a personality right derived from human dignity and intended to protect an individual's moral patrimony, it certainly maintains a very close relationship with the right to honor and, above all, with the right to privacy both declared in Article 18.1 of the Constitution. It should not be forgotten that the capture and publication of an individual's likeness can infringe both upon their right to honor and to privacy. However, the specific character of the right to one's own likeness implies protection against the reproduction of said likeness even if, while affecting the personal sphere of the owner, it does not necessarily damage their good name or reveal aspects of their private life. The right to one's own likeness attempts to safeguard a proprietary and reserved, although not untouchable, domain protected from the intrusions of others; a domain necessary to freely develop one's own personality and, in no uncertain terms, a domain which, made necessary by the strongest traditions of our culture, conserves a minimum quality of human life (STC 231/1988, December 2, FJ 13). This legal asset is safeguarded by the recognition of the authority to prohibit the broadcast, without conditions, of a person's likeness as this constitutes the most important defining characteristic of an individual's personal sphere, inasmuch as basic means of identification and external projection are concerned, and is an essential factor in an individual's self-recognition (SSTC 231/1988, December 2, FJ 3 and 99/1994, April 11, FJ 5).

[19] STC 99/1994, FJ 5

[20] STC 81/2001, FJ 2; STC 83/2002, FJ 5

Given that a person's freedom manifests itself in the physical world through the actions and characteristics of their body, it is evident that, under constitutional protection of an individual's likeness, not only the power to decide how the manifestation of an individual through their likeness is preserved (STC 117/1994, April 25, FJ 3), but also a personal and, in that sense, private sphere of liberty and, as such, the fundamental value of human dignity is also preserved. Therefore, the constitutional role of this right is to allow individuals to decide which aspects of their lives should be protected from public broadcast with the goal of guaranteeing a private domain, free from external interference or the actions of third parties, for the development of one's own personality.[21]

Germany

Basic Law for the Federal Republic of Germany does not include, in these terms, a right to personal privacy or to respect for private life. This does not imply, however, a lack of constitutional protection. Instead, the content of these rights is included in the sphere of protection provided by a more far-reaching basic law: general personality law.

According to Article 2.1 GG, "everyone has a right to the free development of personality as long as they do not infringe upon the rights of others or upon constitutional or moral order."

From Article 2.1, constitutional jurisprudence has extracted two autonomous rights or liberties: general freedom of action (allgemeine Handleitungsfreiheit) and, in conjunction with Article 1.1 GG, general personality rights (allgemeines *Persönlichkeitsrecht*).

The Federal Constitutional Court bases general personality rights on Article 2.2 GG, in conjunction with Article 1.1 GG, which proclaims human dignity and protects human beings, as subjects, against attempts to convert them into simple tools of public authorities.[22]

The Federal Constitutional Court has declared that, *"the function of general personality rights is to guarantee the most intimate sphere of private life and to preserve its basic conditions that cannot be fully protected by traditional liberties."*[23]

It is commonly accepted that the concrete manifestations of general personality rights recognized by constitutional jurisprudence or supported by doctrine, do not fall outside the sphere of protection of the aforementioned fundamental right. The Federal Constitutional Court has reiterated the dynamic character, open to new developments, of the sphere of protection provided by general personality rights intended to protect and guarantee the most intimate private life and its basic conditions *particularly in relation to modern developments and the resulting new threats to human personality.*[24] *The scope of protection cannot be exhaustively determined precisely because it remains open to dangers we are not yet aware of.*[25]

Not all aspects of private life enjoy absolute protection. Constitutional case law states that a preponderant general interest can make it necessary to limit general personality rights when the individual, as a member of a community, comes into contact with others. Their actions influence third parties and therefore affect the personal spheres of others or of community interests.[26] However, there exists, "*an ultimate inviolate sphere, coinciding with private life, absolutely separate from public authority;" "nor can prevalent public*

[21] STC 81/2001, FJ 2

[22] XABIER ARZOZ SANTIESTEBAN, *"Videovigilancia, Seguridad Ciudadana y Derechos Fundamentales",* Ed. Aranzadi, 2010

[23] BVerfGE 72, 155 (170); E 79, 256

[24] BVerfGE 79, 256

[25] BVerfGE 79, 256

[26] BVerfGE 34, 238

interests justify interference in the aforementioned sphere; even if the principle of proportionality is carefully considered. This is partly the result of the guarantee of the essential content of fundamental rights (Article 19.2 GG) and partly due to the fact that the core of personality is protected by unassailable human dignity."[27]

Consequently, the amount of protection provided to private life varies. Constitutional jurisprudence has distinguished two spheres: on one side, an intimate and unassailable sphere, absolutely separate from public authority, and on the other, a protected private sphere into which public authorities may intrude, by legal means, if the greater public good is served and as long as the proportionality principle is followed.

Relevant to the right to one's own likeness, various recent decisions of the German Federal Constitutional Court have been handed down, in the same spirit as those of the Spanish Constitutional Court, relating to the conflict between freedom of information and the right to one's own likeness:

The right to one's own likeness (see BVerfGE 34, 238 (246); 35, 202 (220); 97, 334 (340); 97, 228 (268)) guarantees an individual influence and authority with respect to the capture and use of photographs or images of themselves taken by others. The fact that these photos or images display aspects of private or public life is not in principle relevant. The necessity of protection more accurately arises from –comparable to the right to one's own words which now accompanies the right to one's own image in constitutional jurisprudence (see BVerfGE 34, 238 (246))- the possibility of separating the individual from their image in certain situations, of using it as data and of reproducing it as often as desired for an unforeseen group of people. This possibility has grown more likely due to technological advances which permit the capture of images from great distances, ultimately including from satellites, and under poor light conditions.

As a result of reproduction techniques, the perception of the public spaces in which an individual appears can change. In particular, the visible public space in which one normally moves can be replaced by an environment filled with various forms of electronic media.[28]

France

Similarly, the right to privacy is not explicitly included in the French Constitution of 1958. The French legal system views the right to private life as guaranteed only by civil law. However, Article 9 of the constitution is more closely related to respect for private life more than to the privacy of private life.

Today, faced with new technologies and renewed threats to private life, the right to privacy appears to be little known in France as it has not distinguished itself from similar ideas. Still, the right is very useful and is more adaptable to the changes which have taken place in society in the last few decades.

As such, in 1995 the French Constitutional Council stated[29] that the right to privacy was implicit in the Constitution and later affirmed its statement in 1999[30] when it declared that the liberty proclaimed in Article 2 of the *"Déclaration des droits de l'homme et du citoyen de 1789"* implied a respect for privacy.

The article literally states:

The goal of any political association is the protection of natural and imprescriptible human rights. These rights are liberty, ownership, security and resistance to oppression.

Liberty is defined as the ability to do anything that does not harm others. As such, the only limits to the exercise of the natural rights of the individual are those that guarantee that other members of society enjoy the same rights. These limits can only be determined by law (Article 4 of the Declaration of the Rights of Man and of the Citizen of 1789).

---

[27] BVerfGE 34, 238, E 80, 367

[28] BVerfGE 101, 361 (381)

[29] Decision 94-352DC of the Constitutional Council, January 18, 1995

[30] Decision 99-416DC of the Constitutional Council, July 23, 1999

On June 3, 2009, the Senate Committee publicized a report on the right to privacy in the digital age ("*La vie privée à l'heure des mémoires numériques"*). One of the 15 recommended improvements[31] to the guarantee of privacy against digital threats was the inclusion of the right to privacy in the French Constitution. However, on June 10, 2009, the president of the CNIL (*La Commission nationale de l'informatique et des libertés*) confirmed that it is not very likely that the Constitution would be modified to that end in the next few years.

The consecration of the right to one's likeness is based on Article 9 of the Civil Code which, by simply affirming that *everyone has a right to their private life,* has revealed itself as *"a framework for personality rights."*

In spite of the abundant civil case law on the subject, the right to one's image did not emancipate itself from the right to a private life until a recent decision by the Court of Appeals[32]. Unintentionally signaling the possible changes to come, the decision noted that the right to one's own likeness and the right to privacy can be distinguished by the fact that the former focuses on the reproduction and representation, in a visible and recognizable manner, of the human form. There are also numerous examples in which unauthorized recording of a person's private moments, published without authorization, violates both the right to one's likeness and the right to privacy.

However, the spheres of influence of these rights should not be confused because of the existence of infractions against the right to one's own likeness. These infractions are no more than the recording in public places, including during daily life, of an individual's likeness with the intention of publishing it without consent. Consequently, the right to one's own likeness can be easily invoked independently of the right to privacy in order to protect the individual's personality when it is expressed in public activities. It is distinguishable from the right to privacy because it seeks to protect the individual from misrepresentation in the public eye.[33]

Belgium

Following the example set by the Spanish Constitution, the Belgian Constitution of 1994 expressly stipulated in Article 22 that:

Every individual shall have the right to respect of their private and family life except in those situations and under those circumstances established by the law.

The law, the decree or the provision established by Article 134 shall guarantee the protection of this right.

Holland

The Dutch Constitution, in its 2008 revision, granted citizens an explicit right to private life. According to its Article 10:

1. *All individuals have the right to respect of their personal privacy within the boundaries established by, or in virtue of, the law.*
2. *Parliamentary Law shall establish standards in order to protect privacy with regards to the storing and dissemination or broadcast of personal data.*
3. *The right of the individual to be informed of the stored information concerning them and of its use, in addition to the right to correct it, shall be regulated by law.*

[31] French Senate Issues Report on the Right to Privacy in the Digital Age, "Privacy and Information Security Law Blog, Hunton & Williams, LLP, June 11, 2009

[32] Cass. Civ. 1st, May 10, 2005, Informations rapides (IR), p. 1380: the Court does not mention a right to one's image but rather "due respect for the image."

[33] A. Bertrand, Droit a la vie privee et droit a l´image, Paris, 1999, p. 133

In 2009, the results of an evaluation of the Dutch Constitution were published. The evaluation concluded that the scope of protection of privacy had changed under the aegis of the European Convention on Human Rights and its interpretation by the European Court of Human Rights. However, it was also noted that in the Netherlands less importance was currently given to privacy. This change can be principally attributed to the terrorist attacks of Sept. 11, 2001 in New York but, from a more general point of view, Dutch public opinion had changed with regards to privacy. This change mainly originated from a willingness to relinquish privacy in favor of security.

Poland

The Polish Constitution of 1997 recognizes the right to privacy and protection of information. According to its Article 47:

All individuals have a right to legal protection of their private and family life, of their honor and good reputation and to make decisions concerning their personal affairs.

However, as with other constitutional rights and liberties, the enjoyment of the right to privacy can be subject to certain limitations whenever:

1. They are imposed by law only.
2. They are necessary for the protection of security and public order in a democratic state.
3. They do not in any way violate the spirit of recognized basic constitutional rights and freedoms.

Greece

The Greek Constitution of 1975 recognizes the right to privacy and to confidential communications. According to its Article 9:

1. *The home is considered a sanctuary. An individual's private and family may not be violated. No home may be searched, in any way, except in those cases, and in the manner, established by law. Searches must always be carried out in the presence of representatives of the judiciary.*
2. *Those who violate the aforementioned precept shall be charged with violation of the sanctuary of the home and with abuse of authority and shall be responsible, as indicated by law, for any damages suffered by the injured party.*

Italy

Even though the Italian Constitution, passed in 1948, protects privacy of communication and of the home it does not explicitly mention an independent or autonomous right to privacy. As such, the legal statute concerning privacy is derived from the constitutional provisions that imply its existence as suggested by the case law of the Italian Constitutional Court in Decision/Judgment No. 38 of April 14, 1973.

Among the most relevant provisions, Article 2 of the Italian Constitution states:

The Republic recognizes and guarantees certain unassailable human rights, be it as an individual or in social groups expressing their personality, and insures the fulfillment of the unalterable obligation of political development and economic and social solidarity.

Article 14 later states:

1. *The home may not be violated.*
2. *Inspections or searches may not be carried out except in those cases and in the manner established by law and must conform to guarantees laid out to safeguard personal liberty.*
3. *Special laws regulate verifications and inspections carried out for public health and safety reasons or for economic or fiscal purposes.*

Article 15 also states:

1. *Liberty and the confidentiality of correspondence, or of any form of communication, may not be violated.*

2. *Restrictions on them may only be placed, when sufficient grounds exist, by legal authority and in accordance with guarantees established by law.*

The legal statute regarding privacy, understood as the right to obtain an exact and complete representation of an individual's *"personal identity"*, is also based on Article 3 of the Italian Constitution which states:

All citizens have the same social status and are equal before the law regardless of gender, race, language, religion, political opinion or personal or social conditions. It is the responsibility of the Republic to eliminate any economic and social obstacle that, through the restriction of the liberty and equality of citizens, impedes an individual's full development or the participation of all workers in the country's political, economic and social structure.

The United Kingdom

The United Kingdom does not have a written constitution. The Human Rights Act of 1998 stipulated a limited incorporation of the European Convention on Human Rights into the country's national legislation (including the right to privacy). This act came into effect October 2, 2000. Up to now, courts have enacted the new legislation cautiously. A common law right to privacy is slowly appearing in trust law cases (various trust laws have been used since 1849 to protect against the unauthorized dissemination of personal information).

2.3 THE RIGHT TO PROTECTION OF DATA

2.3.1 EXTENT OF THE PROTECTION OFFERED TO THE RIGHT TO PROTECTION OF DATA IN COMPARATIVE LAW

Spain

According to paragraph 4 of Article 18 of the Spanish Constitution:

The law shall limit the use of computer in order to guarantee the honor and individual and family privacy of citizens and the full exercise of their rights.

According to constitutional case law, this guarantee, recognized in Article 18.4, constitutes a fundamental right with both an instrumental and an autonomous dimension. The instrumental dimension arises strictly from the wording of Article 18.4 which establishes:

…the institutional guarantee of other rights: fundamentally honor and privacy.[34]

The second dimension deduced from Article 18.4 CE refers to a fundamental autonomous right which is:

…in itself an institutional right or freedom: the right to freedom from potential aggression against dignity and individual liberty arising from the illegitimate use of mechanized data processing or that which the Constitution refers to as "informatics".[35]

[34] STC 254/1993, FJ 6

[35] STC 254/1993, FJ 6

This conception is more clearly explained in STC 11/1998:

Article 18.4 *not only carries within it a specific instrument for the protection of the rights of the citizen against the unjust use of computer technology, as has been said, but also enshrines a fundamental autonomous right to control the flow of information concerning an individual's privacy, according to the definition used in the Exposition of Motives for the Regulatory Organic Law on the Automatic Processing of Personal Data (la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal), whether or not it strictly falls within the sphere of privacy, in order to protect the unhindered exercise of his or her rights. This represents an attempt to avoid the facilitation of discriminatory actions by the use of computers in the processing of information.*[36]

This fundamental autonomous right is based precisely on an individual's ability to control the flow of information that concerns him: the right to consent to the gathering and use of personal data, the right to be aware and be notified of the purpose for which said information is destined and the right to access, rectify and erase that data.

The Constitutional Court has noted that:

The guarantee of an individual's private life and their reputation today possesses a positive dimension which exceeds the sphere of the fundamental right to privacy (Art. 18.1 CE) and translates to a right to control of data relative to the individual themselves. So-called "computing freedom", as such, is a right to control the use of the very data inserted into a computer program (habeas data) and includes, among other aspects, a citizen's ability to oppose the use of certain personal data for purposes different from those used to justify its collection (SSTC 11/1990, FJ 5 and 94/1998, FJ 4).

This fundamental right to the protection of data, contrasted with the right to privacy of Art. 18.1 CE, with which it shares the objective of offering an effective constitutional protection for private and family life, grants the individual a set of abilities principally based on the legal authority to obligate third parties to carry out or refrain from certain actions whose strict regulation is established by law. According to Article 18.4 CE, an appropriate law must limit the use of computers to process personal data and as such should strengthen the fundamental right to protection of data (Art. 18.1 CE) and facilitate its exercise (Art. 53.1 CE).

The purpose of the fundamental right to the protection of data is, therefore, the regulation of the manner in which data, extracted from the sphere of an individual's personal, private and family life, is obtained, used and stored. This is also the intent of the fundamental right to data which grants an individual the legal authority to decide if personal data should be made public (STC 292/2000) and it is the keystone of the constitutional and legal protection of data: an individual's ability to fully control the use and destination of his or her personal data.

From this foundation the principles which close the loop, informed consent and purpose, are derived. Except in cases stipulated by law, an individual's personal data can only be used with his or her consent and only if he or she is fully aware of the data to be used, the purpose of its use and his or her rights (access, rectification, cancelation and opposition). Similarly, use of data shall always be conditional on the interested party's knowledge of the explicit, unequivocal, determined and legitimate purpose for which it is used.[37]

According to STC 292/2000:

---

[36] STC 11/1998, FJ 5

[37] XABIER ARZOZ SANTIESTEBAN, *"Videovigilancia, Seguridad Ciudadana y Derechos Fundamentales",* Ed. Aranzadi, 2010.

Above all, the substance of the fundamental right to the protection of data is the power granted to an individual to decide which data they are willing to provide to a third party, be it the State or an individual, or which data a third party may request. This allows the individual to know who possesses their personal data and for what purpose it is being used and enables him or her to oppose that possession or use. This authority to control personal data, part of the substance of the fundamental right to protection of data, has its legal foundation in the ability to grant access to personal data, consent to its acquisition and collection or permit its use or possible use by a third party, be it the State or a private individual or organization. Furthermore, this right to grant access to personal data or to consent to its processing, with or without the use of computers, absolutely requires, on the one hand, the ability to know who can access personal data and to what end it is being used and, on the other, the ability to oppose that access and use.

In conclusion, the right of interested parties to be aware of, and consent to, the collection and use of their personal data are characteristic elements of the constitutional definition of the fundamental right to protection of personal data. Recognition of an individual's right to be informed of who possesses their personal data and for what purpose, and the right to oppose that possession and use, which requires those concerned to terminate these activities, is indispensable if the right is to carry any weight. This is to say, the titular owner of a data resource is required to inform all interested parties of what data pertaining to them has been stored and to grant them access to available registries and resources. They are also required to inform interested parties of what is being done with their data, including any transfers to third parties, and, if necessary, to correct or erase incorrect data.

Effectively, an individual deprived of the ability to control their personal data is also robbed of their fundamental right to the protection of data, given that, as concluded in STC 11/1981 of April 8 (FJ 8), the essential content of the right is bypassed or ignored when it is subject to limitations which make it impossible or unreasonably difficult to exercise or strip it of the necessary protection (FJ 10).

The Constitutional Court has enthusiastically affirmed that the right of individual to be informed as an essential element of the fundamental right to protection of personal data. Obviously, an individual cannot control what is done with their personal data if they are unaware that a third party possesses it or is in a position to use it. Therefore, it is vital, for the effective guarantee and respect for the right of interested parties to be informed of who possesses their data, why and what for, to know the possible destination or uses of their personal information. Furthermore, this knowledge allows interested parties to react to the gathering and use of their information by exercising their right to oppose the processing of data and to the rectification and erasure of data.

STC 292/2000 (FJ 13) highlights the following:

As such, without the guarantee implied by the right to information obtained in accordance with established legal requirements (Art. 5 LOPD) an individual's right to control their personal data would not carry any weight. Clearly, they would impede the exercise of other powers which form part of the content of the fundamental right to which we refer.

Germany

In a decision reached on February 23, 2007, German constitutional case law clarified the constitutional implications of the use of video surveillance in relation to the fundamental right to informational self-determination. The Court argued:

1. *The projected installation of video surveillance interferes with the general personality right of the plaintiff from the perspective of the right to information self-determination. The right to informational self-determination includes the ability of the individual to freely decide when and to what extent information from their personal life is made public and to freely determine the release*

and use of personal data. Images recorded through video surveillance can and should be used to take restrictive measures against individuals who display certain undesired behaviors in the area monitored. Video surveillance of a public place not done in secret can and should act as a deterrent and should discourage undesirable behavior (see Geiger, Verfassungsfragen zur polizeilichen Anwendung der Videoüberwachungstechnologie bei der Straftatbekämpfung, 1994, p. 52). Through the recording of images, observed actions are stored and can be later discharged, processed and exploited especially in relation to other data. In this manner, a variety of information concerning certain distinguishable actions is obtained and can, in extreme cases, take the form of behavioral profiles of affected individuals in the monitored area.

Interference with fundamental rights does not cease because only actions in public places are recorded. The general personality right not only guarantees protection of the private or intimate sphere but also, in the form of the right to informational self-determination, protects an individual's interests, with regards to the protection of information, when they are in public (see BVerfGE 65, 1 (45)).

It cannot be presumed that consent has generally been given to record information exclusive to the intrusion when those affected have been notified by means of a sign that they are being filmed in the spatial area of a public place. The absence of express protest cannot be equated to declaration of consent (see VGH Baden-Württemberg, Decision of July 21, 2003; Decision of July 10, 2003 of the State Constitutional Court of Saxony).

2. *The right to informational self-determination can be restricted in favor of a greater good. However, this requires a legally clear and proportional precedent corresponding to that mandated by the rule of law.*

The Constitutional Court has made it clear that the installation of video surveillance capable of recording images is not excluded and can be wholly constitutional if it has a sufficiently clear and precise legal precedent, there is sufficient motive for it and the surveillance and recording of images respects the proportionality principle, in particular in the spatial and temporal sphere and also in relation to the possible use of the data acquired.[38]

France

The right to protection of personal data is not expressly enshrined by constitutional provisions. However, since the *Prevención de la corrupción* decision of 1993, the abusive handling of personal data has been indirectly prohibited. In that decision, the Constitutional Council took the position that the mechanism established on January 6, 1978 by Law no. 78-17 (relative to the processing of data by computers, files and liberties) plays a role in the protection of individual freedom.

Insofar as the scope of protection of personal data is concerned, the nature of the information in question is unimportant. It is enough that it directly or indirectly names an individual. The information need not be of interest mainly due to its personal nature.

From the point of view of the legal system, the protection of personal data is viewed first as a right of access, second as a limit on sharing and, lastly, as a way to control the purposes for which data is processed and as a right to rectify or erase data.

Holland

The second paragraph of Article 10 of the Dutch Constitution states that "*Parliamentary Law shall stipulate the rules for the protection of privacy in relation to the register and dissemination / broadcast of personal*

[38] XABIER ARZOZ SANTIESTEBAN, *"Videovigilancia, Seguridad Ciudadana y Derechos Fundamentales",* Ed. Aranzadi, 2010.

data. (3) The right of individuals to be informed of stored data concerning them and the way in which that data is used, along with the right to rectify that data, shall be governed by law."

Poland

Article 51 of the Polish Constitution states:

1. *No one can be obligated, except by law, to reveal private information.*
2. *Public authorities may not acquire, compile or access the private information of citizens any more than is necessary in a democratic state under the rule of law.*
3. *Everyone has the right to access official documents and compiled data concerning them. The limitations of this right shall be stipulated by law.*
4. *Everyone has the right to demand the rectification or suppression of false or incomplete information or of information gathered by unlawful means.*
5. *The principals and procedures for accessing and collection of information shall be stipulated by law.*

Greece

A constitutional amendment in 2001 added a new provision to Article 9 granting individuals a direct right to the protection of their personal information. Article 9A states, *"Everyone has the right to be protected from the collection, processing and use, especially by electronic means, of their personal data as specified by law"* The article stipulates that, *"the protection of data be guaranteed by an independent authority established and operated according to law."*

Belgium, Italy and the United Kingdom

A review of the constitutional texts of EU member states shows us that not all of their constitutions include a right to the protection of personal data. Member countries of the EU can be split into three categories: those that expressly recognize the right to protection of personal data as an independent right in their constitutional texts, those that include it as a consequence or a derivation of the right to privacy and those do not refer to it all. Belgium, Italy and the United Kingdom are examples of this last category. However, the inclusion of the Charter of Fundamental Rights of the European Union in the collective law of the EU has granted the right to protection of personal data autonomy at the constitutional level throughout Europe.

3 DATA PROTECTION REGULATION IN EUROPE

Information and communication technologies vastly increase the speed at which information can be processed, storage capacity and the quantity of data transmitted. An enormous amount of information is constantly in circulation without the knowledge of interested parties. This intense global processing of personal data threatens basic human rights and reduces the individual's sphere of privacy. Accordingly, the need to grant specific protection from new threats has led to the development of ad hoc rules in the majority of legal systems in Europe.

Modern automated processing of personal data has received special attention from international and European Community law and the domestic law of member states. Along with the evolution of the so-called information society, a broad debate has arisen around existing policies regarding protection of data and around the most appropriate strategies for safeguarding this right.

3.1 CONVENTION NO. 108, OF JANUARY 28, 1981, OF THE EUROPEAN COUNCIL

The concern of supranational organizations for respect of privacy rights and for the social disorder that new technologies can cause is embodied by Convention 108 of the European Council. The objective of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (Art. 1).

These words establish a series of basic principles for the protection of data and set criterion for regulating its flow. It also creates an advisory committee responsible for the formulation of proposals for facilitating the application of the convention.

The convention includes, in its second chapter, some basic principles for the protection of data: the principles of legality, accuracy, purpose, pertinence, non-abusive use, the right to removal, public access, individual access, security and protection from the automatic processing of data that reveals race, politics, religious or other convictions or is relative to health or sexual preference (except when adequate guarantees are provided by law).

The most important articles for the purposes of this report are those which constitute the legal foundation for subsequent international and domestic regulations with regards to protection of data.

Preamble

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend safeguards for everyone's rights and fundamental freedoms, and in particular the right to respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

Chapter I – General provisions

Article 1 – Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2 – Definitions

For the purposes of this convention:

- ***a.*** *"personal data" means any information relating to an identified or identifiable individual ("data subject");*

Chapter II – Basic principles for data protection

Article 4 – Duties of the Parties

1. *Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.*
2. *These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.*

Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

- *a. obtained and processed fairly and lawfully;*
- *b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;*
- *c. adequate, relevant and not excessive in relation to the purposes for which they are stored;*
- *d. accurate and, where necessary, kept up to date;*
- *e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.*

Article 6 – Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7 – Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8 – Additional safeguards for the data subject

Any person shall be enabled:

a. *to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;*
b. *to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;*
c. *to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;*
d. *to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.*

Article 9 – Exceptions and restrictions

1. *No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.*
2. *Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:*
    a. *protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;*
    b. *protecting the data subject or the rights and freedoms of others.*
3. *Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.*[39]

This convention can be summarized by the principals it establishes: those that are understood to be absolutely necessary for member States that have ratified it.

3.1.1 FOUNDATIONAL PRINCIPLES OF THE CONVENTION

The Principle of Legitimate Purpose: Before a databank is activated, the purpose for its creation must be specified and must be verifiable at any time:

a) If the collected and stored data relates to the objective for which the databank was created (the pertinence of data).
b) If the information is used for a purpose different from that of the databank (the principal of non-abusive use).
c) If data is not kept any longer than is necessary to achieve the objective for which it was initially stored (the principle of removal).

The Principle of Legality: The collection of data must be carried out by legal means.

[39] http://www.apd.cat/media/246.pdf

The Principle of Accuracy: All those responsible for a databank are obligated to verify the accuracy of stored data and to ensure it is up-to-date.

The Principle of Public Access: A public registry of automatic databanks must be available.

The Principle of Individual Access: Everyone has the right to know if data concerning them is subject to computer processing and, if it is, to receive a copy of the data. This includes the right to rectify erroneous or inaccurate data.

The Principle of Security: Databanks must be protected wherever they may be.

3.2 DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL OF OCTOBER 24, 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA

The legislative disparity between member States and the insufficiency and the ambiguity of Convention 108 made it necessary to establish a more concrete and detailed set of rules which would serve as common ground, within the European or supranational sphere, from which data and fundamental rights could be protected.

Based on the first paragraphs of convention, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was passed on October 24, 1995. It established a framework for a coordination of applicable national legislations on the subject of protecting data in order to guarantee its free movement between member States. The principles of protection of an individual's rights and freedoms, specifically respect for privacy, contained in the directive strengthened those of the convention, taken, as they are, from its Article 11.

The result was an equivalent protection enjoyed by all citizens throughout the Union. The 15 member States of the EU were asked to modify their national legislations in accordance with the directive before October 24, 1998.

The directive applies to *any operation or set of operations which is performed upon personal data* referred to as data processing. These operations include the collection, recording, transmission, etc. of personal data. The directive also applies to data processed automatically and to data stored or intended to be stored in data filing systems accessible according to specific criteria.

The directive does not apply to data processed in the carrying out of exclusively personal or domestic activities and does not extend to public security, defence or criminal law. These subjects are not within the scope of Community law and, as such, remain under national legislation. However, as the member States have used Directive 95/46/EC as a basis for their laws regarding data protection, its content is fundamental to them (there is a common tendency to apply, with various limitations and exceptions, the principles found in the directive to police regulations or to those regulations relative to the use of video surveillance by State Security Forces and Law Enforcement Agencies).

The directive specifies the principals and requirements that must form part of a minimum standard of adequate protection. This refers to two types of principals: those which are taken into account when data is gathered and those which are taken into account when data is handled or processed.

3.2.1 PRINCIPLES RELATIVE TO THE ACCURACY OF DATA WHEN IT IS GATHERED

Article 6 of the directive makes use of, in essence and almost word for word, the content of Article 5 of the 1981 convention:

1. Data must be processed in a legal manner and must remain true to its original form (**the principle of legality**).
2. The purpose for which data is gathered must be specified, explicit and legitimate. This restriction also applies to any subsequent processing (**the principle of purpose**).
3. Data must be appropriate and pertinent to and not excessive for the purpose for which it is requested or subsequently processed (**the principle of pertinence and of non-abusive use**).
4. It must also be accurate and, whenever necessary, brought up to date. Inaccurate or incomplete data must be rectified or erased (**the principle of accuracy**).
5. Lastly, data must be stored, in a manner allowing the identification of interested parties, for a period of time not longer than that necessary for the purpose for which it was gathered or subsequently processed (**the principle of removal**).

3.2.2 PRINCIPLES RELATIVE TO THE ACCURACY OF DATA WHEN IT IS PROCESSED

When data is handled or processed, the **principles of confidentiality** (Art. 16), **security** (Art. 17) and **consent of interested parties** (Art. 7) must be observed. Interested parties also benefit from **the principle of access and opposition** (Art. 12 and 14).

For illustrative purposes, the principle sections of Directive 95/46/EC have been included here. As has been said, they are the regulatory pillars supporting the protection of data at the European level and the inspiration behind relevant domestic law.

1. *Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;*
2. *Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;*

(…)

9. *Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for maneuver, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for maneuver and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;*
10. *Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;*
11. *Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;*

(…)

13. *Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;*
14. *Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;*
15. *Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;*
16. *Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;*

(…)

68. Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

Article 1 - Object of the Directive

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.

Article 2 - Definitions

For the purposes of this Directive:

a) 'personal data' shall mean 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;

b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Article 3 - Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Directive shall not apply to the processing of personal data:
    - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

(…)

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:
    a) processed fairly and lawfully;
    b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
    c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
    d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
    e) 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. Member

States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II - CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(…)

(e) 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;

SECTION V - THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12 - Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

a) without constraint at reasonable intervals and without excessive delay or expense:
   - confirmation as to whether or not data relating to him are being processed and information at least 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,
   - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
   - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

b) (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

c) (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI - EXEMPTIONS AND RESTRICTIONS

Article 13 - Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
g) the protection of the data subject or of the rights and freedoms of others.

SECTION VII - THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14 - The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

4 LEGISLATION ON THE PROTECTION OF DATA IN EUROPEAN COMPARATIVE LAW

As far as data protection is concerned, member States' domestic laws closely conform, albeit on the basis of various legislative proposals, to Directive 95/46/EC. This directive lays out the foundational principles of the right to protection of data.

These include, with respect to the ever greater role played by computer technology in society:

- Data should be gathered in a legal and just manner
- Data should be gathered and processed for a specific legitimate purpose
- Data should be appropriate and pertinent to, and not excessive for, its purpose (the proportionality principle). It should be accurate and up-to-date.
- Data should be stored for a limited time appropriate to its purpose (the principle of the right to removal)
- Consent should be given by the data subject (except in cases stipulated by law)
- Data should be transmitted only to those for which it is intended or to legally authorized third parties (the confidential nature of information)
- Data should be handled in a secure manner
- The rights of the individual should be respected (the right to be informed of the collection and use of data, the right to oppose the collection of one's data and the right to access and rectify data)

In the following table, the national data protection laws can be easily seen:

Country	National Data Protection Legislation
Spain	LO 15/1999 of Dec. 13, 1999 on Protection of Personal Data[40]
Germany	Federal Data Protection Act Stand: 1. January 2002 as of 1 January 2002 [41]
France	LOI no 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1)[42]

[40] http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html

[41] http://www.uaipit.com/files/documentos/0000004276_Federal%20Data%20Protection%20Act.pdf

[42] http://www.uaipit.com/files/documentos/0000006347_Loi801_datos_caracter_personal_2004_08_06.pdf

Holland	Personal Data Protection Act of Nov. 23, 1999 (Consolidated Version Apr. 5, 2001)[43]
The United Kingdom	Data Protection Act, Jul 1998[44]
Austria	Federal Act concerning the Protection of Personal Data [45]
Belgium	Loi relative à la protection des données à caractère personnel du 8 décembre 1992. [46]
Denmark	Act No. 429 of 31 May 2000. Act on Processing of Personal Data[47]
Greece	Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended by Laws 2819/20001 and 2915/20012)[48]
Ireland	DATA PROTECTION ACT, 1988 [49]
Italia	LEGGE 31 dicembre 1996, n. 675. Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. [50]
Portugal	Lei Nº 41/2004, Transpõe a Directiva Nº 2002/58/CE, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. [51]
Sweden	Personal Data Act (1998:204) [52]
Norway	Lov om behandling av personopplysninger (personopplysningsloven) [53]

Table 1: National Data Protection Laws

[43] http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml

[44] www.legislation.gov.uk

[45]http://www.uaipit.com/files/documentos/0000005395_Ley_de_Proteccion_de_Datos_Personales_17_08_1999(en_ingles).pdf

[46]http://www.uaipit.com/files/documentos/0000004281_personal%20data%20protection.pdf

[47] http://www.uaipit.com/files/documentos/0000004291_Act%20on%20Processinf%20of%20Personal%20Data.pdf

[48] http://www.uaipit.com/files/documentos/0000004306_Ley%202472.pdf

[49] http://www.uaipit.com/files/documentos/0000004627_DATA%20PROTECTION%20ACT.pdf

[50] http://www.uaipit.com/files/documentos/0000000572_F1-IS-IT-Decr675-19961231.htm

[51]http://www.uaipit.com/files/documentos/0000005637_Ley_47_transposicion_direciva_datos_personales_2004_08_18.pdf

[52] http://www.uaipit.com/files/documentos/0000004339_Personal%20Data.pdf

[53] http://www.uaipit.com/files/documentos/0000004478_The%20Personal%20Data%20Act.pdf

5 PRACTICAL ADVICES IN DATA PROTECTION FOR ELASSTIC COMPLEX

What is PERSONAL DATA?

Under EU Law as well as under CoE law, personal data are defines as information relating to an identified or identifiable natural person.[54]

Form of appearance of the data could be:

- Written or spoken communications, images, CCTV footages or sound
- Electronically recorded and stored information

Both convention 108 (Art. 6) and the Data Protection Directive (Art. 8) name categories of personal data

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions, religious or other beliefs
- Personal data concerning health or sexual live

Users of personal data, may be.

Controller

Whoever decides to process personal data of others, if several persons take this decision together, they may be “joint controllers”

Data controllers are the people or body, 'which determines the purposes and the means of the processing,' both in the public and in the private sector.

Data controllers are required to observe several principles. These principles not only aim to protect the data subjects but also are a statement of good business practices that contribute to reliable and efficient data processing.

The Rules are:

- Data must be processed fairly and lawfully.
- They must be collected for explicit and legitimate purposes and used accordingly.
- Data must be relevant and not excessive in relation to the purpose for which they are processed.
- Data must be accurate and where necessary, kept up to date.

[54] Data Protecion Directive, Art. 2 (a); Convention 108 Art. 2 (a)

- Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them.
- Data that identifies individuals must not be kept longer than necessary.
- The Directive states that each Member State must provide one or more supervisory authorities to monitor the application of the Directive. One responsibility of the supervisory authority is to maintain an updated public register so that the general public has access to the names of all data controllers and the type of processing they do.
- In principle, all data controllers must notify supervisory authorities when they process data.
- Member States may provide for simplification or exemption from notification for specific types of processing which do not entail particular risks. Exception and simplification can also be granted when, in conformity with national law, an independent officer in charge of data protection has been appointed by the controller.
- Member States may require prior checking, to be carried out by the supervisory authority, before data processing operations that involve particular risks may be undertaken. Which types of processing operations involve particular risks is for the member states to determine.

Processor

Is a legally separate entity that processes personal data on behalf of a controller. Anybody who receives data from a controller is a “recipient”

Third party

Is a natural or legal person who does not act under instructions of the controller

Basic for processing of personal data is the consent of the person affected, as stated in the Data Protection Directive (Art. 2 h), “any freely given specific and informed indication of the data subject´s wishes”. The elements of valid consent are:

- Free (not been under pressure)
- Informed (the person knows data might be gathered and processed and knows about the objective and consequences of consenting)
- Specific (the person knows reasonably concrete what type of data is gathered/processed and which use it is going to give)

Likewise, the right to withdraw consent at any time is critical.

5 CONCLUSION

The EU has a policy that one must be tolerate throughout its territory, and whose basic principles have to be respected by the national laws.

This directive (Directive 95/46/EC) lays out the foundational principles of the right to protection of data.

- Data should be gathered in a legal and just manner
- Data should be gathered and processed for a specific legitimate purpose
- Data should be appropriate and pertinent to, and not excessive for, its purpose (the proportionality principle). It should be accurate and up-to-date.
- Data should be stored for a limited time appropriate to its purpose (the principle of the right to removal)
- Consent should be given by the data subject (except in cases stipulated by law)
- Data should be transmitted only to those for which it is intended or to legally authorized third parties (the confidential nature of information)
- Data should be handled in a secure manner
- The rights of the individual should be respected (the right to be informed of the collection and use of data, the right to oppose the collection of one's data and the right to access and rectify data)

6 BIBLIOGRAPHY

ETXEBARRIA GURIDI, JOSE FRANCISCO, "Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados", Ed. Tirant lo Blanch, 2011.

REBOLLO DELGADO, LUCRECIO, "Derechos Fundamentales y Protección de Datos", Ed. Dykinson, 2004.

SUBIZA PÉREZ, IGNACIO, "La Protección de Datos y sus mundos", Ed. DAPP, 2009.

ARZOZ SANTIESTEBAN, XABIER, "Videovigilancia, Seguridad Ciudadana y Derechos Fundamentales", Ed. Aranzadi, 2010.

GONZÁLEZ URDINGUIO / GONZÁLEZ GUTIERREZ DE LEÓN, «La videovigilancia en el sistema democrático español. Análisis crítico de la Ley Orgánica 4/1997, de 4 de agosto», Revista de la Facultad de Derecho de la Universidad Complutense, núm. 89, 1998, p. 105 y ss.

ULL SALCEDO, M.V., «El derecho a la intimidad como límite a la videovigilancia» en Revista de Derecho Político, núm. 63, 2005, pp. 177 y ss.

ROXANA CALFA Y SPERBER SEBASTIAN, Ciudadanos, ciudades y videovigilancia "Hacia una utilización democrática y responsable de la videovigilancia" Foro Europeo para la Seguridad Urbana, Bourgeois. 2010

RODOTÀ STEFANO, "Democracia y protección de datos ", Cuadernos De Derecho Publico, Ministerio De Administraciones Publicas 2003

LUCAS MURILLO DE LA CUEVA, PABLO "La Constitución y el derecho a la autodeterminación informativa", Cuadernos De Derecho Publico, Ministerio De Administraciones Publicas 2003

PIÑAR MAÑAS, JOSE LUIS, "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", Cuadernos De Derecho Publico, Ministerio De Administraciones Publicas 2003

CERVERA NAVAS, LEORNARDO, "El modelo europeo de protección de datos de carácter personal", Cuadernos De Derecho Publico, Ministerio De Administraciones Publicas 2003

TÜRK ALEX, Presidente de la Comisión Nacional de Informática y Libertades (CNIL), Francia, "La ley francesa de protección de datos de carácter personal", Junio 2005.

OLESTI RAYO, ANDREU, "Las Políticas de La Unión Europea relativas al Control en las Fronteras, Asilo e Inmigración", ReDCE, nº 10, Julio-Diciembre de 2008

FERNÁNDEZ ROZAS, J.C., "El espacio de libertad, seguridad y justicia consolidado por la Constitución Europea", Revista Jurídica Española La Ley, 2004, 4, D-195, pp. 1867-1881.

AGUELO NAVARRO, PASCUAL, "Schengen, fronteras que unen" 2006.

DEL VALLE GÁLVEZ, ALEJANDRO, "Las Fronteras de la Unión - El Modelo Europeo de Fronteras"

GRAS, MARIANNE L. "The Legal Regulation of CCTV in Europe" Surveillance & Society CCTV Special (eds. Norris, McCahill and Wood), 2004

PÉREZ-CRUZ MARTÍN, AGUSTÍN-JESÚS, "Videovigilancia y Derecho a la Intimidad: ¿Un nuevo ejemplo de conflicto entre el Derecho a la Seguridad Pública y el Derecho Fundamental a la Intimidad?.

CANALES GIL, ÁLVARO, Interventor Ex-Subdirector General de Inspección de Datos, "El Derecho Fundamental a la Protección de Datos de Carácter Personal", REVISTA JURÍDICA DE CASTILLA Y LEÓN. N.º 12. ABRIL 2007 13

HERRÁN ORTIZ, ANA ISABEL, "La evolución jurídica del concepto de intimidad a la luz del desarrollo tecnológico", Ed. Vlex.

EUROPEAN UNION AGENCI FOR FUNDAMENTAL RIGHTS , "Handbook on European data protection law ", 2013

This project has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement no 312632.

http://cordis.europa.eu/fp7/cooperation/home_en.html

http://ec.europa.eu

PROJECT PARTICIPANTS:
ARCADIS NEDERLAND BV (NL)
FRAUNHOFER-INSTITUT EMI (DE)
INSTITUTO CONSULTIVO PARA EL DESARROLLO SL (ES)
JA JOUBERT ARCHITECTURE (NL)
NORTH BY NORTH WEST ARCHITECTES SARL (FR)
SCHÜBLER-PLAN INGENIEURGESELLSCHAFT MBH (DE)
SIEMENS AG (DE)
TNO – NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (NL)
UNIRESEARCH BV (NL)