DELIVERABLE

Project Acronym: SMARTSPACES

Grant Agreement number: 297273

Project Title: Saving Energy in Europe's Public Buildings using ICT

Deliverable D9.1

Ethics and Data Protection Framework

Authors:

Werner B. Korte	EMPIRICA	Jan van Hess	VENLO
Eriona Dashja	EMPIRICA	Roddy Black	BRISTOL
Georg Vogt	EMPIRICA		
Radmilo Savic	BELGRADE		
Nigel Godfrey	BIRMINGHAM		
Paul Isbell	BRISTOL		
Wilfried Ponischowski	HAGEN		
Mustafa Aliç	ISTANBUL		
Nick Morris	LEICESTER		
Emili Loncà Aventin	LLEIDA		
Fernando Iannone	MILAN		
Hélène Chessel	MOULINS		
Eduardo de San Nicolás Juárez	MURCIA		

Project co-funded by the European Commission within the ICT Policy Support Programme		
Dissemination Level		
P	Public	x
C	Confidential, only for members of the consortium and the Commission Services	

REVISION HISTORY AND STATEMENT OF ORIGINALITY

Revision History

Revision	Date	Author	Organisation	Description
0.1	May-12	Georg Vogt	empirica	Initial draft
0.2	Jun-12	Eriona Dashja Georg Vogt	empirica empirica	Work on content
0.3	Jun-12	Radmilo Savic Nigel Godfrey Paul Isbell Wilfried Ponischowski Mustafa Aliç Nick Morris Emili Loncà Aventin Fernando Iannone Hélène Chessel Eduardo de San Nicolás Juárez Jan van Hees	Belgrade Birmingham Bristol Hagen Istanbul Leicester Lleida Milan Moulins Murcia Venlo	Contribution of partners
0.4	Jul-12	Eriona Dashja Georg Vogt	empirica empirica	Drafting document
0.5	Jul-12	Radmilo Savic Nigel Godfrey Paul Isbell Wilfried Ponischowski Mustafa Aliç Nick Morris Emili Loncà Aventin Fernando Iannone Hélène Chessel Eduardo de San Nicolás Juárez Jan van Hees	Belgrade Birmingham Bristol Hagen Istanbul Leicester Lleida Milan Moulins Murcia Venlo	Revision by partners
0.9	Jul-12	Wilfried Ponischowski Roddy Black	Envi Bristol	Peer review
1.0	Jul-12	Eriona Dashja Georg Vogt	empirica empirica	Final edit

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Table of Content

List of Figures

1 Introduction

Data Protection is addressed in SMARTSPACES project as it is a relevant if not key issue that needs to be dealt with at all pilot sites. It is against this background that the project team has developed a template document to collate data protection requirements in each pilot site regarding the services to be provided as definitions taken from the Data Protection Directive. Specific instructions were included in the template to facilitate partners' understanding on the subject in order to provide clear information coherent with all other project steps.

The current document aims to:

- Support pilot site partners on the implementation of a data protection policy.
- Encourage the good implementation of the Data Protection Directive.
- Document different practices in Europe. This would enable future SMARTSPACES services users to select and implement the data protection policy that fits best with their situation.

At the same time, a close follow up of data protection requirements in each pilot site will be carried out and potential issues arising discussed in consortium meetings. Any outcomes of ethics management beyond the results presented in this deliverable will be reported in the framework of exploitation deliverables.

Work carried out in this deliverable is based on the collection of requirements in WP1. The deliverable D1.1 ("Requirements for SMARTSPACES services and Systems") summarises requirement groups (see section 2.2.5) and individual requirements (see chapter 3.1.5) relevant for data protection management. Chapter 5 of the Deliverable 1.1 also provides first information on Data Protection, confidentiality, safety and nature of personal data, as well the impact of the Directive 95/46 on SMARTSPACES project overall.

The current document presents an updated version of chapter 5 and includes an introduction to the context of Data Protection. Chapter 2 summarizes the Data Protection framework to be used in SMARTSPACES. Chapter 3 gathers the Data Protection legislation in pilot countries and if applicable further guidance on pilot level.

2 The SMARTSPACES ethics and data protection framework

2.1 Conceptual approach

The objective of determining the provision of information on energy consumption to users and to staff is to identify the primary domains of legal and regulatory relevance to the planned services. As a result, an overview of the practices and requirements of the energy measurement and information in the participating countries is given in SMARTSPACES D1.1, as well as a comparison of EU member states' situations and a breakdown of the forthcoming constraints that will enable SMARTSPACES partners to better anticipate coming requirements linked to EDSS and EMS solutions. Data Protection is an important issue when making data publicly available and needs to be addressed at all pilot sites.

The Data Protection Directive 95/46 has a direct impact on the implementation of the EDSS and EMS solutions of the SMARTSPACES project. The envisaged services are focused on improving employees' resource management services involving personal data on their consumption behaviour. However, not all the information collected is personal data, therefore the pilot sites need to define the type of information they will manage during the project.

SMARTSPACES partners are considered as controllers in each participating country. The collection, processing and transmission of personal data must be analysed under the principles of Directive 95/46/CE and especially the respective National laws. Any additional regulations at National level that are not in the Directive and apply to Data Protection or any other sensitive information are also taken into account for SMARTSPACES project development.

The data collected for the development of SMARTSPACES services are generally not considered personal data as they do not refer to a natural person. A template is proposed to SMARTSPACES partners in order to identify if the involved data is considered personal or not (SMARTSPACES D1.1, pp. 120).

This chapter presents the framework on data protection and ethics as to be used in SMARTSPACES.

2.1.1 Data privacy in service operation

In modern societies, the interest in the right of privacy particularly increased with the advent of information technology. Today, all European Member States have put some kind of data protection legislation in place which sets out specific rules covering the handling of electronic data. This may include a general law that governs the collection, use and dissemination of personal information by both the public and private sectors. It may also include sector-specific laws governing data protection in relation to specific domains such as health care, employment and so on. In general, data protection provisions tend to describe personal information as data that are afforded protection at every step from collection to storage and dissemination. Basic principles that have frequently been enshrined into legislation include that personal data are obtained fairly (e.g. not violating informational self-determination) and lawfully (e.g. consent-based); that they are used only for the original specified purpose; that they are adequate, relevant and not excessive to purpose; that they are accurate and up to date as well as accessible to the subject and that they are kept secure and destroyed after its purpose is completed.

2.1.2 Data privacy in evaluation

In SMARTSPACES, a user survey has to be conducted before the realisation of the services and after the realisation of the services. Surveys should be conducted in formalized way at all pilot

sites. Various issues need to be treated with care so that anonymity of the survey is ensured and that users understand the need to collect information.

When planning a survey, besides the general approach (longitudinal or cross-sectional study) the following two topics are particularly relevant:

- The willingness of respondents: How to motivate tenants to participate in a survey?
- The content of questionnaires: How to operationalise the aspects of interest?

Motivating the respondents for the participation in the survey is a very important issue, because the response rate has to be maximized in order to do sophisticated analyses or analyses for subgroups.

According to experiences of survey research, several strategies and instruments can help to raise the willingness of the focus groups to participate:

- The choice of field instrument. There are different field instruments to conduct a survey (postal/paper-based; telephone interview, face to face interview, online survey). In general a more personal form of conducting the survey will raise the motivation to participate and will lower the non-compliance of the respondents.
- The layout and content of the cover letter or introduction text. An introduction to the survey for the respondents is necessary.
- Number and content of reminders / re-visits. Every reminder / re-visit will increase the response rate. In general, up to 3 reminders / re-visits are recommended. The first one can take place 7-10 days after the first invitation.

The anonymity of the survey should be protected by using IDs and associated means of assuring privacy of the personal data.

2.1.3 Ethical issues in SMARTSPACES

No ethical issues have yet been identified for the project or by the partners. The ethics and data protection manager will report regularly on the status and necessary activities of partners during consortium meetings. Further outcomes of ethics management are to be reported in the framework of exploitation deliverables.

2.2 SMARTSPACES project guidelines

Following, more operational guidance is provided on how the ethical perspectives discussed above will be adhered to within the SMARTSPACES project. This starts with a summary given in the table below, followed by more specific guidelines to be adopted for the purposes of the project. In the following subsections, more specific guidance is provided on how compliance with the ethics and data protection requirements summarised in the table above is to be achieved within the project.

Figure 1 - Key Issues in Data Protection and Ethics Management

Theme	Key issues	Operational guidance
Data protection in Operation / Evaluation	Data privacy is to be guaranteed during all stages of the project according to European and national standards.	A review of national data protection regulation/legislation will be conducted across the eleven pilot sites' countries, and project activities at each pilot site will comply with these respectively. Pilot sites are to adhere to general data protection guidelines prepared by the project in relation to piloting/evaluation activities.
Ethics	No ethical issues have yet been	The ethics and data protection

	identified.	manager will report regularly on the status and necessary activities of partners during consortium meetings. Further outcomes of ethics management are to be reported in the framework of exploitation deliverables.

2.2.1 Specific guidance on data privacy

All pilot sites are to follow a common data protection protocol as follows:

- Only authorised research/other personnel within the participating organisations should be granted access to data.
- All data must be made to be anonymous.
- Only summaries of the quantitative data should be available. Excerpts (e.g. quotations) from the qualitative data may be included in any results section of any report or academic publication.
- Participants must be treated with respect at all times and their anonymity protected. Pseudonyms or codes must be used to replace any identifiers within the data. Every quotation must be made anonymous using e.g. a pseudonym or ID.
- Quotations from interviews for publicity purpose (e.g. in a case study, reports and publications) can be attributed if consent has been given.
- Reports must only contain selected passages of interview transcripts and must not publish transcripts in their entirety. All quotations will be made anonymous.
- If participants wish to talk to interviewers about sensitive issues which they wish to remain confidential, interviewers must not use what they hear in this context in any part of the research.
- Personal paper-based details of participants must be kept in locked filing cabinets.
- Transcription must be made anonymous.
- Data (transcripts, audio and video recordings) will be kept in locked cabinets.
- Interview/focus group recording, transcription and analysis: It is essential that data is made to appear anonymous. Reference numbers must be used to identify tapes, transcriptions and data analyses.
- All information that could be used to identify the participant (names, address, and personal details) must be separated from the data permanently before analysis.
- Participants have the right to prevent data processing that is likely to cause damage to themselves or anyone else.
- Video recordings of persons will also be separated from identifiers permanently and will not be used publicly, unless the participant has given consent in writing that (parts of) the video can be used for publicity purposes.

If consent of individual users is required the following issues need to be considered:

- In which way the consent is given/ collected?
- Is it possible to withdraw the consent?
- Is the explanation of the consent given, of the service and the way to withdraw sufficiently transparent?

Beyond this generic protocol, each pilot site must comply with national data protection legislation/regulation.

2.2.2 Confidentiality and safety of the personal data processing

The personal data managed by the SMARTSPACES project must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

The partner in charge of the data processing must respect the following obligations:

- The data should not be kept in a form which permits identification of individual users.
- Respect the purposes for which the data was collected or for which it is further processed.
- Ensure appropriate protection for personal data stored for longer periods for historical, statistical or scientific use.
- Certify the security of collected personal data, which should be kept safe and secure from potential abuse, theft, or loss.
- Draw up contracts with all subcontractors to ensure that they respect the data processing and protection obligations such as they exist in the legislation of the Member State.

2.3 Ethics and data protection management

Ethics and data protection management activities during the first year focused to a large extent on analysing ethics and data protection requirements that are to be applied to the project, and on developing operationally useful guidance in terms of the SMARTSPACES ethics and data protection framework presented throughout this document.

The ethics and data protection manager will report regularly on the status and necessary activities of partners during consortium meetings. Further outcomes of ethics management are to be reported in the framework of exploitation deliverables.

3 Legal and regulatory background

This chapter provides an overview of the legal and regulatory background on the Data Protection Directive and its impact on SMARTSPACES project. Furthermore, it presents specific requirements and details on data protection issues that are part of national legislation in pilot member states, and their applicability in SMARTSPACES pilot sites.

3.1 Regulatory / legislative framework at the European governance level

Rapid developments in technology have dramatically increased the scale of data sharing and collecting so bringing new challenges in the area of personal data protection. Considering the importance that building trust in the online environment has on economic and social development, the European Union has established a regulation for personal data protection in the Union. The existing EU legislation on personal data protection (Directive 95/46/EC), adopted in 1995, intends to protect the fundamental right to data protection and guarantee the free flow of personal data between member states. Currently, a proposal is being discussed for a revised data protection directive which is briefly discussed in this section.

3.1.1 Data protection directive

The European Union Directive 95/46/EC for Data Protection is the official document that has the objective of the protection of individuals with regard to the processing of personal data and on the free movement of the data obtained. The Directive represents an important component of EU privacy and human rights law.

The Data Protection Directive addresses punctual definitions for the identification of personal data and derived parties involved in the data collection, which are (Art. 2 a-h, Directive 95/46/EC):

- Personal data "any information relating to an identified or identifiable natural person; 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;"
- Processing "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;"
- Personal data filing system ”any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.”
- Controller “a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by National or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by National or Community law.”
- Processor “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.”
- Third party “ any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.”

- Recipient “a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.”
- Data subject's consent “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.”

The principles of the Directive are honesty and transparency, legitimate purpose and proportionality in order to guarantee the free flow of data within the EU. As a result of the Data Protection Directive, European Union member states have implemented legal dispositions to protect the personal data of their citizens and the following basic principles for processing personal data have to be followed in all Member States:

- **Honesty and Transparency:** The data subject has the right to be informed when his or her personal data are being processed. The controller must provide his or her name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. Data may be processed only under the following circumstances :
  - when the data subject has given his or her consent
  - when the processing is necessary for the performance of or the entering into a contract
  - when processing is necessary for compliance with a legal obligation
  - when processing is necessary in order to protect the vital interests of the data subject
  - when 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
  - when processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject

The data subject has the right to access all data processed about him or her. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules.

- **Legitimate purpose**: Personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes.
- **Proportionality**: Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be 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; The data should not be kept in a form which permits identification of data subjects for 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. When sensitive personal data (including religious beliefs, political opinions, health, sexual orientation, race, membership of past organisations) are being processed, extra restrictions apply.

3.1.2 Impact of the Directive 95/46 on SMARTSPACES project

The Data Protection Directive has a direct impact on the implementation of the project's EDSS and EMS solutions. The envisaged services are focused on improving users' resource management service involving personal data of their consumption behaviour. However, the information collated is not always subjected as personal data and it is to pilot sites to define the type of information they will manage during the project.

The collection, processing and transmission of personal data must be analysed under the principles of Directive 95/46/CE and especially of the national laws taken for its application. Any additional regulations at national level that are not in the Directive and apply to data protection or any other sensitive information are also taken into account for SMARTSPACES project development.

Regarding the Directive's principles, honesty and transparency refer to informing the data subject that their personal data is being used. Therefore, data managed during the SMARTSPACES project must be processed only under the following preconditions which need to be met (Art. 7, Directive 95/46/EC):

- When the data subject has given her/his consent
- When the processing is necessary for the performance of or the entering into a contract
- When processing is necessary for compliance with a legal obligation
- When processing is necessary in order to protect the vital interests of the data subject.

The rights of the users from whom information has been collected are the:

- Right of access to collected information
- Right of correction of this information
- Right of opposition to the collection and the processing, in particular right of opposition to the processing at ends of commercial campaigns or use by third parties and to the transfer.

Another principle that applies to the SMARTSPACES project is the legitimate purpose, which implies that personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes.

Processing can only be carried out if the user gives her/his consent, meaning a "demonstration of free, specific, and informed will by which the person concerned accepts that personal data relating to her/him is the subject of a data-processing".

From this principle, there is the possibility of derogation whenever the treatment is "necessary for the conclusion of a contract to which the person is a part" (and, consequently, consent was given by implication). This question requires an examination of national rules which concern the transposition by the Member States.

3.1.3 Current EC-proposal for a revised data protection directive

Since the Directive 95/46 was firstly introduced, Data Protection Acts have frequently been amended by legislation with substantial changes especially during 2009 and 2010 widely driven by the essential changes in ICT related technology. In fact, the law on Data Protection is about to undergo the most fundamental change in 15 years. On 25 January 2012, the European Commission officially presented a first draft of the new data protection regulation for a comprehensive reform of the 1995 data protection rules on personal data processing across the European Union. Once the proposal passes into law, through the European parliamentary system, it will replace the existing Data Protection Act and will require organisations operating in or with the EU to make significant changes concerning the way how they deal with personal data processing

and use. The new EU regulation is scheduled to replace the existing Data Protection Act by 2014 at the earliest, as the European Commission has set a two-year timetable for the implementation of this proposal through the parliamentary system. This draft regulation mainly aims to:

- Promote greater harmonisation of data protection across the EU through a single European legislation As the Directive has not been consistently implemented across the EU member states, significant differences are observed in their national laws. The new regulation, when implemented, will apply directly across all the EU, and the member states would not need to transpose the new measures by implementing their own local law in each jurisdiction. Consequently, companies operating in more than one EU country would no longer need to cope with the national regulation of each member state. Within the new regulation framework, the current provisions set by member states for national reasons would also disappear.
- Introduce a single data protection regulator for the businesses processing personal data across the EU. International businesses will only have to deal with the data regulator of the country where the company has its main establishment instead of dealing with each data regulator in each member state. The draft proposal of the new regulation includes also guidelines on how to identify the main establishment of the company. Citizens would still be allowed to address complaints to the regulatory authority in their country of residence, this is in order to prevent negative impacts on the level of citizens' privacy protection.
- Make the data processors share equal responsibilities. The new regulation shall apply to any data processor in the European Union and also to those outside the Union which offer goods and services to the EU citizens.
- Restrict the use of personal data. Before organisations process data, they should require in advance and on an opt-in basis the consent to use personal information. The age for requiring parental consent is proposed to be the 13 years of age. According to the new draft regulation, individuals will have the right to demand from an organisation to transfer information held about them to a third-party organisation, in a format determined by the individual.
- Increase fines and duties for the companies. For repeated breaches and serious violations the supervisory authorities will impose penalties up to €1 million or up to 2% of a company's global annual turnover. For less serious violations the fines will vary from €250,000 up to 0.5% of turnover. For not supplying information to a user or when not having rectified data the fines are up to €500,000 or up to 1%. The new EU regulations extends administrative duties for the companies, such as: an additional transparency obligation (Article 14); an unlimited right to information (Article 15); drafting corporate guidelines (Article 11); and complex documentation (Article 28). Smaller organisations are put in a better position under the new proposed draft regulation. The obligation to have a data protection officer applies to all public authorities and all businesses employing more than 250 employees, and does not apply to organization with more than 10 employees as stated before.
- Set up a new obligation for reporting data protection breaches. The concept already exists in some EU jurisdictions, such in Germany and Ireland. The draft regulation states that in cases of any personal data breach, the data controllers should notify their relevant data protection supervisory authority within 24 hours, or explain the reasons for not being able to explain the full details of the breach. Separate requirements include notification of data subjects.
- Introduce two new data subject rights for data processors. – The draft regulation introduces the 'right to be forgotten' and the 'right to data portability'. The current data protection already contains legislation regarding the right of the data subject "to be forgotten", and the new regulation draft develops some further specifications related to this issue. To strengthen this right in an online environment, the draft regulation expands the right to erasure and gives to the individual the right to require to a data controller, who has made

personal data publicly available, to stop processing their personal data and to cease all marketing by also informing third parties which are processing that data whenever a data subject requests them to erase it. The right to data portability is the right of the data subjects to require and obtain a copy of their own personal data. In the cases when data subjects provide their data to automated processing systems, they would be allowed to transmit that data from one automated application into another one.

The data protection manager will follow the development of the Directive and inform the consortium in meetings if action is required.

3.2 National Legislation in pilot member states

This section presents relevant national legislation in pilot member states and selected key markets.

Austria

Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 – DSG 2000) Austrian Federal Law Gazette part I No. 165/1999. Amendments: Federal Law Gazette I No. 136/2001

The Austrian Data Protection Act dates from 1978, long before the implementation of the Directive 95/46/EC. In order to ensure that Austria complied with the new requirements set in the Directive in the Directive, the Austrian Data Protection Act 2000 (Datenschutzgesetz 2000 or the DSG) was passed in 1999. This Act came into force on 1 January 2000. Data protection laws to implement the Directive have been adopted by all nine Austrian Länder. Beside the general laws related to the collection and use of personal data, there also sector-specific laws which regulate specific aspects of the collection and use of personal data (e.g. The Austrian Telecommunication Act, The regional data protection laws of the Austrian federal provinces) and some legal provisions are also included in the Austrian Labour Relations Acts, Banking Act, Trade Regulations Act, Criminal Procedure Code, and Police Act. The legislation aims to provide the right to data protection to everyone, including natural persons, (public or private) legal entities and associations (referred to as data subjects).

Article 2 (Part 1) of the Act provides general provisions and definitions concerning data protection issues. With the term “Data” is meant “information relating to data subjects who are identified or identifiable”. “Data Subject”, is defined as “any natural or legal person not identical with the controller, whose data are processed”. “Controller” is a “natural or legal person, group of persons or organ of a territorial corporate body or the offices of these organs, if they decide alone or jointly with others to use data, without regard whether they use the data themselves or have it done by a service provider”. With “use of data” is meant “all kinds of operations with Data, meaning both processing of data and transmission of Data”. The Federal Act, besides personal data, also regulates “sensitive data” (information about a person relating to radical or ethnic origin, political opinions, health, etc.) and provides some provisions about “indirect data” (personal data which can be identified if the identity of the data subject can be retraced, but not by legal means.)

Austrian Data Protection Commission (Österreichische Datenschutzkommission), is the regulatory Authority responsible for the surveillance and enforcement of compliance according to the data protection regulations of the Act. The Commission has the power to make regulations on data protection issues and it also rules on all requests for information.

France

Law 2004-801 of 6 August 2004 modifying Law 78-17 of 6 January 1978

Legislation relating to personal data and computer files was present in France since the late 1970s, with the Law Nr. 79-17 of 6 January 1978. The French Data Protection Authority (CNIL) was set up at the same time by the same Act. After a long legislative process, the directive 95/96/EC was

finally incorporated into French Law with Law Nr. 2004-801 on 6 August 2004, and came into force immediately. The Law relates to the Protection of Data Subjects regarding the processing of Personal Data. The CNIL (Commission Nationale et LIbertés) is responsible for ensuring that information technology remains at the service of citizens, and does not threaten human identity or breach human rights, privacy or individual or public liberties. At the moment there is no specific law in force for energy consumption data protection.

The penalties for data controllers in case they breach the Law are covered in the Article 45 of the 2004 Law. These include fines, imprisonment, ceasing processing operations and removing the controller's authorisation to process. When publishing the case information into newspapers or other forms of publishing, the sanctioned person must pay.

Germany

The Federal Data Protection Act (Bundesdatenschutzgesetz) adopted in 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May 2001.

Data protection law was introduced in Germany long before the introduction of EU Data Protection Directive (95/46/EU). Considering the comprehensive nature of the existing data protection system, implementation of the Directive did not require radical changes. The implementation process of the EU Data Protection Directive (95/46/EU) was finalised on 23.05.2001 through The Federal Data Protection Act. The Act deals with the handling and processing of personal data aiming to protect the individual against his right to privacy. It has been frequently amended by the legislation especially in 2009 and 2010, when the most substantial modifications were made.

The purpose and scope of this act is specified in Section 1. It states that the "Act shall apply to the collection, processing and use of personal data" to the "public bodies of the Federation" and to the "public bodies of the Länder (states) in so far as data protection is not governed by Land legislation and in so far as they (a) execute federal law or (b) act as bodies of the judicature and are not dealing." The Act shall apply also to the "private bodies in so far as they process or use data in or from data files in the normal course of business or for professional or commercial purposes." With "personal data" is meant "any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)" (section3). Further in section 3 by "Collection" is meant "the acquisition of data on the data subject, by "Processing" "the storage, modification, communication, blocking and erasure of personal data", and "any utilization of personal data other than processing" is meant by "use".

As the Federal Republic of Germany is a federation of 16 states, and all of them with their own original sovereign rights and legislative responsibilities, there exists a patchwork of laws and regulations covering data protection in these 16 German states which work alongside the Federal Data Protection Act 2001. A number of different authorities responsible for making sure the compliance of data protection laws and regulation are present in Germany, this resulting from the division of the supreme power of the State between the federal and the state governments. The States are responsible for the data protection supervision in the private sector, except the telecommunications and postal services companies that are monitored by the federal government, and more concretely by the Federal Data Protection Commissioner. In fact, the states have no uniform system concerning the private sector supervision as the supervisory functions are performed by different authorities in different states. Concerning the public sector in the states, supervision of compliance with data protection is under state government responsibility which has assigned this function to independent supervisory authorities (data protection commissioners). The Federal Data Protection Commissioner is responsible for monitoring the compliance of data protection laws and regulations by the federal authorities and other public bodies under the federal government control.

Italy

Personal Data Protection Code (Legislative Decree no. 196 of 30 June 2003)

The Directive 95/46/EC was transposed into the Italian Law on 31 December 1996 with the Act No. 675. This Act, which entry in force on 08 May 1997, provided only the general regulatory framework that applied to data protection which has after been supplemented by a number of later acts. The Personal Data Protection Code in Italy, which came into force on 1 January 2004, brought together all the laws and regulations that were previously governing data protection. The Code aims to ensure that the processing of personal data is done by "respecting data subjects' rights, fundamental freedoms and dignity", especially with regard to "confidentiality, personal identity and the right to personal data protection" (section 2). According to the Section 5, the Code applies only to the "processing of personal data carried out by natural persons for exclusively personal purposes if the data are intended for systematic communication or dissemination." The provisions stated in the Sections 15 and 31 of the Code concerning liability and security apply in any case. The Articles 36-39 of the Act no 675 of 1996 provide details on punishments in cases when data controllers beach the law. They include fines, and also the risk of imprisonment.

Italian Data Protection Commission is the supervision authority in Italy, responsible for supervision of compliance with data protection regulations in the country. Its legal basis is stated under Section 153 of the 2003 Law and its tasks are included in the Section 154 of the same Law.

Netherlands

Law on protection of personal data (Wet Bescherming Persoonsgegevens)

This law provides rules and privacy criteria for keeping and processing personal data. It has existed since 2001, when it replaced the old law of personal registrations (WPR). WBP protects the person whom the data concerns and the duties of the parties who use the data. The WBP relates to every use - 'processing' - of personal data, from the collection of this data up to and including the destruction of personal data. According to WBP personal data is data that contains information relating to a real person and that person is identifiable. The legislation actually applies to 'paper' records, but also offers an adequate legislative framework for a digital record. The law further states that the usage of data should be based on an informed consent of the person and that it should be given by free will. In article 25 a code of conduct for the use of personal data in research is offered. The purpose is to support Dutch universities that conduct scientific research.

The Dutch Data Protection Authority (CBP) supervises compliance with legislation regulating the use of personal data. The CBP primarily supervises compliance with and application of the Dutch Data Protection Act [Wet bescherming persoonsgegevens (Wbp)], the Police Data Act [Wet politiegegevens (Wpg)] and the Municipal Database (Personal Files) Act [Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA)].

Serbia

Law on Personal Data Protection, "Official Gazette of RS", no. 97/2008, 104/2009

The Law on Personal Data Protection came into effect on 4 November 2008 and has been applied since 1 January 2009. This law aims to "ensure realisation and protection of the right to privacy and other rights and freedoms regarding personal data processing to every natural person." By personal data is meant "any information concerning a natural person" regardless of: the data format it exists (paper, tape, film, electronic, etc.); the form in which it is expressed; whose name or account it is stored in; the mode of information learning; the place where it is stored; the original date; and regardless also of other information characteristics (article 3). The individual to whom the personal data relates and who is identified, or identifiable by references, is defined as the natural

person. Personal data processing is considered to be any action performed upon data, such as: “collection, recording, transcription, multiplication, copying, transmission, retrieval, organisation, storage, separation, crossing, unification, adaptation, alteration, provision, use, making available for insight, disclosure, publication, dissemination, revealing through transmission and otherwise making available, hiding, dislocation and otherwise making unavailable, as well as undertaking other activities regarding the aforementioned data, regardless of whether it is being performed automatically, semi-automatically or in other manner”. The only exceptions to the Law are: data which are publicly available; data processed for personal needs and not available to third parties; data on members of political parties, trade unions, associations, etc. when the consent of the members is given; and data published on oneself by a person capable of taking care of their own interests.

The state authority responsible for the supervision of the Law implementation is the Commissioner for Information of Public Importance and Personal Data protection (article 54). The competences and the Commissioner’s powers in supervision are included in the Article 54 and 56 respectively.

Spain

Personal Data Protection Law(1999) ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data(Organic law 15/99)

The protection of personal data is enshrined in the Spanish Constitution through Article 18.4 which requires that the law shall restrict the use of data in order to protect the honour and the personal and family privacy of Spanish citizens, as well as the full exercise of their rights. This provision was further developed by Organic Law 5/1992 on the Regulation of the Automatic Processing of Personal Data, as amended by Organic Law 15/1999 on the Protection of Personal Data. This law corresponds to European legislation. In the Royal Decree 1720/2007, the Rule Development of Personal Data Protection Law is approved. This Decree aims at regulating possible risks of Personal data treatment.

Turkey

In Turkey there is not yet a specific law or regulation which covers the data protection issues in the country. Constitution together with a variety of general laws which are part of the Turkish basic law, criminal law and civil law, govern the data protection in Turkish law. Recently, there exists a draft on personal data protection introduced by Turkey as part of the process for joining the European Union. A specific data protection law is currently part of the parliament’s agenda.

United Kingdom

The Data Protection Act of 1998

The EU Data Protection Directive (DPD) was transposed into national legislation by the Data Protection Act of 1998. The act stipulates general rules for processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Vital signs data is classified as "sensitive personal data" (section 1). "Data protection principles" are set out in Schedule 1 (section 4). As in DPD, "Processing" includes any storage ("holding") or transmission; the data do not have to be manipulated for their use to qualify as "processing". Schedule 1 specifies the first such data protection principle, for the case of sensitive personal data, as "Personal data ... shall not be processed unless ... at least one of the conditions in Schedule 2 is met, and ... at least one of the conditions in Schedule 3 is also met."

Schedule 2 allows processing under at least three circumstances; processing is allowed if

- The data subject has given his consent to the processing.

- The processing is necessary ... for the performance of a contract to which the data subject is a party, or ...
- ... in order to protect the vital interests of the data subject."

Schedule 3 allows processing if consent is obtained i.e. if the data subject has given his explicit consent to the processing of the personal data.

So in summary, the Act allows transmission and storage of vital signs and therefore vital signs triage by anyone, given the client's consent.

Schedule 2 also allows processing if "6 (1) ... necessary for ... legitimate interests pursued by the data controller ... except where the processing is unwarranted" and allows the Secretary of State to specify what this means.

However the Data Protection Act of 1998 covers personal data to a large extent. In relation to data on energy consumption in buildings etc. there are 2 further pieces of legislation: The Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

3.3 Codes of practice, guidelines and quality standards on pilot level

Some cities have additional codes of practice, guidelines and quality standards regarding data privacy. If codes or guidelines are applicable they are briefly introduced below.

Belgrade

The city has numerous data guidelines to be followed by the staff and applicable in SMARTSPACES. The processing of personal data is forbidden in cases when:

- A person has not given permission to use his data.
- The goal of data processing is not the one that has been previously defined.
- The goal of processing has not been transparently defined.
- A person’s identity can be discovered after processing.
- The processing methodology is not allowed.
- The data are not necessary for the goal of data processing.
- The number and type of data are not proportional to the goal of processing.
- Data are false, partial, not authentic or expired.

Birmingham

The city has a Data Protection Policy which provides guidelines on data protection and personal data use. The Data Protection Policy of Birmingham City Council aims to ensure compliance with the Data Protection Act 1998. The Information Commissioner, who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with the eight data protection principles of 'good information handling'. These principles include:

- Personal data shall be processed fairly & lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive
- Personal data shall be accurate and, where necessary kept up to date.
- Personal data shall not be kept for longer than is necessary

- Personal data shall be processed in accordance with the rights of data subjects
- Security principle - Protection against unauthorised /unlawful processing
- Transfers outside of the EEA - Requires adequate levels of protection

The Council's obligation is to protect the individual's freedom and to ensure the individual's rights. It is considered to be unlawful when personal data are used to abuse, discriminate or deny access to services. The City Council is committed to ensure a fair, lawful and a non-discriminatory usage of the personal data it holds including: manual/paper records, electronically processed personal data (also information gathered on CCTV systems), and any type of data at any location that are used by or on behalf of the City Council. The obligations and guidelines outlined in the Data Protection Policy of the Birmingham city council apply to "all those who have access to personal data held by Birmingham City Council, whether employees, agency staff, elected members (or other public representatives), trustees, employees of associated organisations or volunteers", and including also the people who "work at home or from home or have remote or flexible patterns of working".

Bristol

The data users must comply with the eight Data Protection Principles of good practice, which underpin the Data Protection Act 1998. These principles include the same guidelines as presented for Birmingham above:

The requirements of the Data Protection Act are also reflected in the Information Security Policy on personal data protection, established by Bristol City Council. As mentioned in the policy statement, Bristol City Council seeks to apply security measures and other appropriate working practices, in order to protect and assure confidentiality and value to all electronically processed information as well as to the paper based. The Information Security Policy shall apply to all members, agents and contractors of Bristol City Council. It is each individuals' responsibility to:"be familiar with current policies related to IT systems and data protection"; "comply with security measures" regarding computer use and data protection; "take action" in order to prevent misuse of data or systems; "report failures of security" to the responsible security administrator. The Council's disciplinary procedure and standards are applied to any officer who fails to comply with the Information Security Policy.

The Information Security Policy of Bristol City Councils provides also guidelines for internet connection and use of electronic information exchange. They aim to: minimise the external interference risks; make sure that connections are used only for Council purposes, and "protect employer and employee from vicarious liability".

Hagen

The city has numerous data protection guidelines which have been visited. However, as no personal data is being recorded none of them applies in SMARTSPACES.

Istanbul

The city has no specific data protection guidelines.

Leicester

The Leicester City Council offers to its staff the possibility to participate in Data Protection trainings. A specific Information Governance Team deals with data protection and freedom of information requests. The Freedom of Information Act (FOIA) makes the activities of public authorities like Leicester City Council more open to the public. It allows people and organisations from anywhere to access a wide range of information the Council holds. Similarly, the Environmental Information Regulations 2004 (EIR) gives a right of access to a wide range of environmental information held by the Council. Environmental information includes information about planning, energy usage, and pollution. It also includes information relating to the state of

land and information about activities which adversely affect the environment. Subject to certain exemptions ("Exceptions" under EIR) the City Council must answer FOIA and EIR requests within 20 working days of receipt by the Authority.

Lleida

Neither Lleida municipality, nor Lleida Energy Agency has any particular regulations on data protection issues, beside the national laws and legal regulations. In accordance with Article 90 of R.D. 1720/2007 of 21 December, which approves the deployment of the Organic Law 15/1999 of 13 December on the protection of personal data, there must be a procedure of notification and management of incidents affecting personal data. In these cases a record should be kept stating the type of incident, the time it has occurred, or where identified, the person making the notification, to whom he communicates, and the effects derived from the corrective measures applied. In any cases when an incident affecting personal data has been identified, the security officer should be notified.

Milan

The Milan City Council published an internal regulation adopting the decisions taken by the Italian Data Protection Authority, on 25 June 2009 and on 19 March 2011, regarding data protection guidelines to be followed by staff and guidelines on employees' protection. The city of Milan, via an online service and in accordance with the Legislative Decree no. 196 dated 30 June 2003, on information of the data subject as well as entity from whom or which personal data are collected (Article 13), will provide the following information for the treatment of personal data: purpose of treatment; method of treatment; nature of treatment; owner and manager of treatment; rights of the user as interested in the treatment.

Moulins

The major principles of current regulations in the city, concerning data protection, only specify the following points:

- Information transmitted by meters must not allow direct identification of the consumer and its location, only the service provider knows how to interpret the data.
- Access to data base containing consumption index is secured and restricted to buildings managers to help reduce energy bills.
- Access to personal data through a web portal for consumers is only possible with a secure connection and with a personal login and password.
- The main issue is to prevent lifestyle habits tracing: it is not recommended to collect data in real time (privacy intrusion) and to compile energy data more often than every 4 hours.
- In case of individual contracts for electricity and gas, it is necessary to obtain written tenants' agreement.

All the above measures concern social housing area and in case of child care centres, there is no specific restriction (no tenants' privacy intrusion).

Murcia

Murcia City Council and all employees are subjected to Organic Law 15/1999. There is an Internal Security Document, as law requires, which explains some aspects of this Law. The purpose of this Security Document is to implement the security and organizational measures to ensure the security of Electronic Personal Data Files, and all treatment centres, equipments, systems, programs and persons involved in processing all personal data of Murcia Municipality. The realization of the Security Document meets the requirements under Article 8 of Royal Decree 994/1999, June, the 11th on Regulation of Security Measures for Electronic Personal Data Files, which indeed regulates the measures to ensure its safety. RD 994/1999 is applicable to all Electronic Files of Personal Data regulated by the Organic Law 15/1999.

There are three security levels applicable to Automated Personal Data Files: high security, medium security and basic level of security, levels that will apply depending on the types of data processed.

- Basic Security: Files containing personal information such as name, address, telephone number, marital status,(baseline data).
- Medium Security: Files containing data relating to administrative or criminal offenses, financial services, information on Treasury, or a set of personal data sufficient to obtain an assessment of the personality.
- High Security: Files containing sensitive data, such as data on health, sex life, political ideology, union membership or religion.

Venlo

The city has numerous data protection guidelines but no specific guidelines or rules have been set up for the management of data protection issues inside the organisation. In case an audit is needed, the use of the compliance tools as provided by CBP is considered. The building in SMARTSPACES was recently constructed and privacy issues resulting from the technology used were considered during planning.