Societal & Political Engagement of Young People in Environmental Issues

D2.3: Guidelines for handling ethical, legal issues, and data protection

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 649493

Document Information

Grant Agreement Number	649493	Acronym	STEP	
Full Project Title	Societal and political engagement of young people in environmental issues			
Start Date	1st June 2015	Duration	30 months	
Project URL	www.step4youth.eu			
Deliverable	D2.3 Guidelines for handling ethical, legal issues, and data protection			
Work Package	WP 2 - Analysis and requirements			
Date of Delivery	Contractual	1 December 2015	Actual	1 December 2015
Nature	R - Report	Dissemination Level	P – Public	
Lead Beneficiary	SAMPAS			
Responsible Authors	Dr. M.Serdar Yümlü, Caner Tosunoğlu, İbrahim Acar, Gonca Kara Demir			
Contributions from	Paula Forbes [ABERTAY], Christodoulos Keratidis [DRAXIS], Panagiota Syropoulou [DRAXIS], Sotiris Diplaris, Symeon Papadopoulos [CERTH], Albert Garcia Macian [MOLLET DEL VALLES], Josue Alonso [VALDEMORO], Trond Bugge [KAIROS]			

Document History

Version	Issue Date	Stage	Changes	Contributor
0.1	30/09/2015	Draft	First draft of Ethical & Legal issues guideline	İbrahim Acar, M.Serdar Yümlü
0.2	10/10/2015	Draft	EU regulatory framework, cloud and environment added	Caner Tosunoglu, Gonca Kara Demir
0.3	05/11/2015	Draft	Received comments from CERTH, ABERTAY, DRAXIS, VALDEMORO, MOLLET DEL VALLES	Paula Forbes, Christodoulos Keratidis, Sotiris Diplaris, Albert Garcia Macian, Josue Alonso
0.4	15/11/2015	Draft	Revised National Regulatory Frameworks	İbrahim Acar, Caner Tosunoğlu
0.5	18/11/2015	Draft	Added STEP Ethical Guidelines	İbrahim Acar, Caner Tosunoğlu, M.Serdar Yümlü
0.7	26/11/2015	Draft	Review comments from Abertay	Paula Forbes, Stefano De Paoli
1.0	30/11/2015	Final	Final revision includes all comments	M.Serdar Yümlü
2.0	08/12/15	Final	List of contributors updated	Christodoulos Keratidis

Disclaimer

Copyright message

Table of Contents

Executive summary

The **Deliverable *D2.3* – *STEP* Guidelines for Ethical, legal issues and data protection** is part of the **Work Package 2 Requirements and Analysis**. The purpose of this deliverable is to present EU level and national based regulatory frameworks for potential ethical issues that may arise in the conduction of the STEP project. Ethical issues presented in this deliverable have been identified by pilot and technical partners and guidelines for the STEP platform are provided. The intended audience for this deliverable is preliminarily the project partners as the work contained in this document will support the implementation of STEP. However the research work conducted for the EU regulatory framework on privacy & data protection, national frameworks of pilot countries, ethical analysis of e-Government, cloud and participation based STEP platform will be of interest for a wider audience (e.g. policy makers, researchers, the public).

In this deliverable ethical issues have been generally identified considering research involving work with human subjects which involves collecting or processing personal data, regardless of the method by which they are/were collected (e.g. through interviews, questionnaires, direct online retrieval etc.). This document also considers non-EU countries based issues involved in pilot phases, issues that may have a negative effect on environment and environment protection and other ethical issues that may arise and are not listed in the Horizon 2020 guidelines.

The ***STEP* Guidelines for Ethical, legal issues and data protection** deliverable provides guidelines, answers to issues and the technical approach that STEP Platform will adopt for the relevant ethical issues specifically for human involvement, personal data privacy & protection, non-EU third countries involvement and environment. The guidelines and the outcome of this deliverable will be also used as an input for the D3.1 *Architecture and Integration Framework Definition Specification*, in design process and development of the platform.

1 Introduction

The aim of **Deliverable 2.3 Guidelines for Ethical, legal issues and data protection** is to identify ethical issues that may arise in the conduction of the STEP project and in particular issues related with privacy and protection of personal data throughout the life of the STEP project, considering both aspects specific to each pilot country (Turkey, Greece, Spain, Italy) and generally valid at the EU level. The deliverable will present EU level and national level regulatory frameworks for potential ethical issues that may arise in the STEP project. Ethical issues presented in this deliverable have been identified by pilot and technical partners and guidelines for the STEP platform are provided. This analysis is done by the STEP project consortium to get an insight on the regulatory issues for data protection, privacy, non-EU countries involvement and environmental protection.

Chapter 2 presents the regulatory framework for data protection, privacy and public participation in environmental issues. It starts with relevant EU Laws concerning data privacy, protection of personal data and electronic communications. This section continues with a special focus on the national legislations which are in place at the country level project pilot locations (Region of Crete (Greece), Locride area (Italy), Mollet del Vallès (Spain), Valdemoro (Spain), and Hatay Metropolitan Municipality (Turkey)). It also considers the public organizations and stakeholders involved, the status of public and young participation and other potential areas which are relevant for the STEP project pilot.

Chapter 3 presents the legal and ethical framework for the involvement of human subjects in the development and testing of the STEP platform.

Chapter 4 and Chapter 5 present the impact of cloud computing in eGovernment services and environmental protection based issues respectively.

Chapter 6 presents ethical guidelines and the technical approach of the STEP platform for consortium members and all stakeholders. It starts with the approach for the protection of personal data, describes the approach for personalized services and anonymous aggregation of data, presents ethics approval processes, explain how collection and processing of data will occur, give insight for web and social media mining component, identified non-EU countries based issues and provides details on rights to be forgotten and to erasure respectively.

Finally, this deliverable concludes with the outcomes of the legal analysis and with the STEP platform **guidelines for handling ethical issues**.

2 Legal Framework for Privacy Protection

The STEP project aims to develop and pilot test a cloud eParticipation SaaS platform, (available as a mobile application and through a web platform), whose goal is to engage Young European Citizens and Public Authorities in decision making about environmental strategies, policies, plans, programmes, laws, and projects. In order to fulfill the objective of the platform, personal data protection and several other ethical and legal issues are analyzed and identified in this deliverable.

Under the European Union (EU) law, personal data is defined as "any information relating to an identified or identifiable natural person" [1]. The collection, use and disclosure of personal data at a European level are regulated in particular by the following directives:

- Directive 95/46/EC on protection of personal data (Data Protection Directive) [1]
- Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) [2]
- Directive 2009/136/EC (Cookie Directive) [3]

Directives generally do not directly apply in the EU and associated non-EU countries and need to be nationally implemented by each country through laws and regulations. As countries have some freedom in the implementation of directives, stricter requirements than those prescribed by the directives may apply in certain EU countries. Furthermore, the national data protection legislation is, in many respects, complemented or overlapped by sector specific legislation that also needs to be considered. Therefore, in order to get a clear and comprehensive picture of the data protection requirements, it is essential to check the national frameworks, national data protection laws, unfair competition legislation, telecommunications laws and any other local data protection regulations.

The use cases for STEP platform in general consist of transactions between different stakeholders involved in the youth/public participation to decision making procedures (Government to Business (G2B), Government to Citizen (G2C), Business to Government (B2G), Citizen to Government (C2G)) which imply transfer/exchange of data/information. Any action that takes place in such e-Government service environments can potentially raise privacy issue, which could be addressed not only through technology but also through the procedures in place. Privacy issues also arise in platform development projects where testing and pilot execution phase exists, as collection of information about individuals, public entities and private organizations will be required.

A crucial aspect of the discussion around personal data processing and protection is related to the deployment of the offered services in a cloud computing environment, as additional risks have to be taken into consideration in this case. The majority of these risks fall within two broad categories:

- Lack of control over the data
- Insufficient information regarding the processing operation itself (absence of transparency).

2.1 EU legal framework for privacy protection

Privacy is enabled by protection of personal data. According to Data Protection Directive (95/46/EC) of the EC, personal data "means 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 of more factors specific to his physical, physiological, mental, economic, cultural or social identity" [1].

The same Directive also defines personal data processing as "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."

There are several legal acts within the EU Law that address and regulate these issues:

- Charter of Fundamental rights of the EU
  - Article 7 states that "everyone has the right respect for private and family life, home and communications"
  - Article 8 regulates that "Everyone has the right to the protection of personal data concerning him or her" and that processing of such data must be "on the basis of the consent of the person concerned or some other legitimate basis laid down by law"

- Directive 95/46/EC (Data protection Directive)

  The Directive regulates the processing of personal data regardless of whether such processing is automated or not. The principle is that personal data should not be processed at all, except when certain conditions are met.

  - Article 6(b): Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."
  - Article 7 defines criteria for making personal data processing legitimate:
    - the data subject has given his consent
    - processing is necessary for the performance of or the entering into a contract the data subject is party
    - processing is necessary for compliance with a legal obligation the controller is subject
    - processing is necessary in order to protect the vital interests of the data subject
    - 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
    - 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.

- **Directive 2002/58/EC (Directive on privacy and electronic communications, also known as e-Privacy Directive)**

  e-Privacy Directive concerns the processing of personal data and the protection of privacy in the electronic communications sector and deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies [2].

- Article 5 Confidentiality of the communications
  - Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
  - Paragraph 1 shall not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.
  - Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

- **Directive 2009/136/EC (Cookie Directive)**

  This Directive amended Directive 2002/58/EC, requiring end user consent to the storing of cookies on their computer. Cookies are hidden information exchanged between an

Internet user and a web server stored in a file on the user's hard disc. They can be used to monitor Internet activities of the user [2].

The Directive states that the measures referred to in paragraph 1 Article 4 of the Directive 2002/58/EC shall at least:

- ensure that personal data can be accessed only by authorized personnel for legally authorized purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data.

2.2 Accessibility and "easy-to-use" principle

Considering the general rights of people to access the information and to participate in decisions about the environment, it is very important that all people have equal access to the tools that enable use of those rights. There are three major cause of discrimination: digital divide, e-Literacy and disability [4].Digital divide is the gap between people who have access to the Internet and those who do not. E-Literacy means level of knowledge and computer skills that enables people to use e-Government services. Lack of computer literacy is serious obstacle for people's participation in e-Government and cause of inequality.

Any kind of disability must not prevent people to use an e-Government service as it is aimed to serve all people irrespective of their physical capabilities.

The EU Law related to the issue is the following:

- Charter of Fundamental rights of the EU (Article 21- non discrimination)

  Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited [12].

- Digital Agenda for Europe COM(2010)245 final
  - It is essential to educate European citizens to use ICT and digital media and particularly to attract youngsters to ICT education
  - There is also need for concerted actions to make sure that new electronic content is also fully available to persons with disabilities. In particular, public websites and online services in the EU that are important to take a full part in public life should be brought in line with international web accessibility standards [Web Content

Accessibility Guidelines (WCAG) 2.0.]. Moreover, the UN Convention on the Rights of persons with disabilities contains obligations concerning accessibility[1].

2.3 Data security

Data should be secure from viruses, hacker attacks, forgery etc. Security means protection of information and information systems by ensuring confidentiality, availability, integrity, authentication, and non-repudiation[2] .

- Confidentiality: Information is not made available or disclosed to unauthorized individuals and entities.
- Availability: Data/information have to be available, only authorized persons can remove it, in accordance to law
- Integrity: only authorized persons can modify the data/information, in accordance to law
- Authentication must be preserved (data/information must be authentic)
- Non-repudiation – participants will not be able to successfully challenge the authorship of the data provided

- Directive 2002/58/EC (e-Privacy Directive):
  - Article 4. Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Council Framework Decision (2005/222/JHA) addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service attacks. The Framework Decision seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can take action against this form of crime. At the moment, there is a proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA.

[1] www.un.org/disabilities/convention/conventionfull.shtml
[2] http://www.dol.gov/_sec/e_government_plan/p23_security_privacy.htm

Table 1 presents the importance of each EU level legislation for STEP platform and how it will be considered in this document.

Table 1 Summary of EU Legislation from STEP perspective

Legislation/Act/Article	Importance for STEP Platform
Directive 95/46/EC on protection of personal data (Data Protection Directive)	• Processing of personal data and collection in STEP platform
Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)	• Protection of privacy in web and mobile based STEP communication channels • Confidetiality of information
Directive 2009/136/EC (Cookie Directive)	• Management of hidden information Exchange between participants and the STEP platform
Accessibility (Article 21)	• Increasing accesibility issues in STEP platform usage among young participants
Data security (2005/222/JHA)	• Confidentiality, integrity, authentication and non-repudiation features to be provided by the platform

2.4 National frameworks

This section describes national frameworks of pilot countries involved in the STEP project and in particular Turkey, Spain, Italy and Greece. National frameworks are identified considering public participation to environmental issues, electronic communication, e-Government applications & policies, the right of access to information and personal data and data protection.

2.4.1 Turkey

Currently, Turkey does not have a specific data protection law. There is a Draft Code on the Protection of Personal Data (Draft Code), which aims to harmonise Turkish data protection laws with the Council of Europe's Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (Data Processing Convention). Turkey has signed but not yet ratified the Data Processing Convention. Likewise, the Draft Code has not been adopted yet.

In the absence of a specific data protection law, general provisions found in various codes regulate data protection as follows.

Turkish Constitution. Following the constitutional amendments of 2010, protection of personal data became an individual right and, as a result, restrictions on recording and processing personal data were introduced:

- Article 17 states that every individual is entitled to rights of living, protection and improvement of his material and spiritual being.
- Article 20 states that everyone has the right to request the protection of his personal data. Personal data can be processed only in accordance with law, or with the concerned individual's consent.
- Civil Code. Articles 23, 24 and 25 safeguard personal rights:
    - Article 23 sets out that no individual can waive his freedom or restrict it contrary to law.
    - Article 24 states that violation of personal rights is unlawful unless justified by the consent of the person whose right has been violated, superior private or public benefit, or authority granted by law.
    - Article 25 also sets out civil remedies in case of infringements of personal rights.

Code of Obligations. In particular:

- Under Article 27, an agreement contrary to personal rights is invalid.
- Under Article 58, a person whose personal rights have been violated can seek damages against the person who has violated those rights.
- Article 419 imposes a duty on an employer in relation to employees' personal data. Accordingly, an employer can only use the employees' personal data in relation to the employee's qualifications or if it is required to perform a service.

Criminal Code. In particular:

- Under Article 134, anyone who violates the secrecy of a person's private life can be fined or imprisoned from one to three years.
    - According to Article 135, the following can subject the offender to a prison sentence of six months to three years for illegal recording of personal data, for the violation of the data recording prohibition, for recording personal data without the consent of the affected party and for illegally recording data relating to the political, philosophical or religious views, ethnic origins, moral inclinations, sex lives, or union affiliations of individuals.
- Under Article 136, illegal transfer, dissemination and collection of personal data is punishable by imprisonment of one to four years.
- Article 138 provides that individuals, who are responsible for deletion of personal data following the expiry of the retention period, can be imprisoned for six months to one year if they fail to fulfil this duty.
- Law on the Right to Access Information. The aim of this law is to promote free access to certain information, but in the meantime it restricts the right to access certain confidential information such as a person's private life or commercial secrets.

There are also other sectoral laws that apply for Labour Law (Article 75), Banking (Card Payment Systems) (Article 73) and for Electronic Communication sectors concering personal data and protection,

According to Article 4, personal data should be processed: In accordance with the law and good faith principles.

- Upon the data subject's consent.
- In relation to its purpose.
- Adequately and proportionately.

Public Participation

The eTransformation of governmental transactions initiative was introduced in 2003, and a national policy was launched towards adaptation to the electronic processing of transactions. In 2008 Law on Electronic Communication enacted (Official Gazette No: 26530). As electronic communication becomes widespread, so do the online crimes, hackings and cyber attacks. Consequently a legislation was enacted on 04.05.2007 on Regulating the Internet Transmission Issues and Combating the Crimes Committed by Internet Transmission. (Law No: 5651, Official Gazette No:26530).

The Right to Access to Information was guaranteed by the Law on the Right to Access Information that was published in the Official Gazette in 2003 (Law No: 4982). However the privacy issues and commercially classified information is protected by regulations such as Regulation on Personal Information Registry and Protection of Privacy, Law on Competition (No:4054 Official Gazette No:) and a Decree on Protection of Commercial Secrets and Access Rules to the Commercial Information (No:2010/3).

Environmental Issues

In Turkey, a legislation for the environment was approved and enacted in 1983, (No.2782, 11.08.1983, OG No: 18132) since then several amendments to the Environment Law have been added, updating the related articles in complying with the new requirements.

Environmental Impact Assessment is compulsory by law in Turkey since 1993. A Regulation was enacted in 2008 on the Environmental Impact Assessment. The regulation clearly defined the involved parties and their roles, rights and liabilities.

2.4.2 Spain

In Spain, the STEP project has two different pilots. The first pilot will be in the Valdemoro district of Madrid and the second pilot in the Catalan region of Mollet del Vallès, Barcelona. Spanish national frameworks are discussed here from the Spanish Law and regional Catalan Law perspectives including Local City Councils decisions related to public participation, electronic communication, e-Government policies, and personal data protection. The classification is done as follows:

- ES: Spanish Law (National)
- CAT: Catalan Law (Regional)
- LR: Local Regulation (City Council)

Different regulatory topics analyzed and identified in Spanish pilot use-cases based on personal data protection and public participation are as follows:

Personal Data Protection

- ES: Law 15/1999, of December 13, Protection of Personal Data. (BOE 14/12/1999). Royal Decree 1720/2007 of 21 December, approving the Regulation implementing Law 15/1999 of 13 December on the protection of personal data is approved.
- ES: Royal Decree 1720/2007, 21th of December, in which the regulation implementing the Organic Law on Protection of Personal Data was adopted
- ES: Law 19/2013, of December 9, transparency, access to information and good governance. (BOE 12/10/2013).
- ES: Law 21/2013, of December 9, Environmental Assessment. (BOE 11/12/2013)
- ES: Law 27/2006, of July 18, by which the rights of access to information, public participation and access to justice in environmental matters are regulated (incorporates the Directives 2003/4 / EC and 2003 / 35 / EC). (BOE 19-07-2006)
- CAT: Law 19/2014, 29th of December, on Transparency, access to public information and good governance
- LR: Law 2/2002, of June 19, Environmental Assessment of the Community of Madrid
- ES: Royal Decree 3/2010, 8th of January, in which the National Security Scheme (ENS) is regulated in the field of eGovernment
- ES: The National Security Scheme (ENS) regulates the communication through electronic administration between citizens and Public Administration and focuses on Data Protection

Public Participation

- ES: Law 27/2006, of July 18, by which the rights of access to information, public participation and access to justice in environmental matters are regulated (incorporates the Directives 2003/4 / EC and 2003 / 35 / EC). (BOE 19-07-2006)
- ES: Law 11/2007 of 22 June, electronic access of citizens to public services. (BOE 23/06/2007). The law on electronic access of citizens to Public Services gives citizens the right to interact electronically with public administrations, and the obligation of these to ensure that right.
- ES: Law 19/2013 , 9th of December, on Transparency, access to public information and good governance
- CAT: Law 19/2014, 29th of December, on Transparency, access to public information and good governance
- LR: Municipal Organic Regulation, adopted on 1995

Both Spanish pilots (Valdemoro and Mollet del Vallès) will apply their own checking mechanisms to sustain ethics and privacy issues during the STEP project. Also at regional level Mollet pilot will adopt regional practices in STEP project.

At National Level (Spain), the National Security Scheme (ENS)[3] will be adopted by both pilot cities, which regulates the communication through electronic administration between citizens and Public administration and focuses on Data Protection. "ARCO rights"[4] (Access, Rectification, Cancellation, Opposition, Objection) regarding personal and sensitive data will be also adopted at National level.

At regional level (Catalan Government), The Catalan Government performs Preventive Audits to Catalan Municipalities randomly and the municipality reports to the Catalan Government (Regional Level) every single Database creation which contains sensitive information. The municipality of Mollet del Vallès hires private companies to audit the City Council regarding personal and sensitive data protection and the degree of fulfillment of the National Security Scheme (ENS) which regulates the communication, through electronic administration, between citizens and Public administration and focuses on Data Protection. The City Council of Mollet del Vallès also assigns a Committee responsible for data protection.

Other specific actions to be taken by Mollet del Vallès pilot are:

- On the 2nd of January the City Hall of Mollet del Vallès will launch a Transparency Portal, which will also include a Public Participation Portal focused on Citizen engagement in the decision making process. The Transparency Portal will be the first experience of Mollet del Vallès on "e-Government cloud-based solutions" before the launch of the STEP platform.
- Capacity Building: the municipality of Mollet del Vallès offers specific training on sensitive data management and protection to civil servants who manage sensitive information

Minors Involvement

The STEP project partners in Mollet del Vallès have a very good existing relationship with several local secondary schools. Although the initial proposal stated that it would not be necessary to involve minors (16-18 yr olds may or may not be classed as minors, depending on the country[5]) the opportunity to have feedback and design input from a group of 16-18 year olds would be of benefit to the project and also helps to strengthen this positive relationship further. This cohort of young people would be likely to be early users of the STEP platform. In order to maintain the integrity of the STEP project, pilot activities will comply with the ethical procedures detailed below:

- Inform parents of the proposed workshop research activity
- Provide detailed information sheets to the young people (and for parents)
- Obtain written informed consent from parents and the young people themselves
- Ensure that participants know their contribution is entirely voluntary and they may decide to withdraw from the research activity if they wish.
- Ensure that the researchers involved in the workshop activity are trained in dealing with non-adult participants

[3] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf
[4] http://www.uoc.edu/portal/en/_peu/avis_legal/drets-arco/index.html
[5] http://fra.europa.eu/en/theme/rights-child/child-participation-in-research

- Ensure that participant information and participant consent documentation is appropriately drafted
- Ensure that Protocols for use of the school or similar settings have been observed

2.4.3 Italy

In Italy protection of personal data is guaranteed by the Italian Legislative Decree 30 June 2003, 196, in compliance with the EU Law. The Law n. 547, 23th December 1993, defines the Criminal Code and the Criminal Procedure Code on the subject of computer crime.

The Law n.150, 7th June 2000, addresses the issue of transparency, acknowledging the right of access of citizens to administrative institutions and to administrative proceedings, including the use of consultation and active participation action. A specific law (Legge Stanca, Art. 4, 9 January 2004) has been defined to face the issue of accessibility, intended as the "ability of computer systems, in the manner and to the extent permitted by technological knowledge, to provide services and usable information, without discrimination, even for those who, because of personal disabilities, require assistive technology or special configurations". The Italian Legislative Decree 7 March 2005, n. 82, the so called "Public Administration Digital Code" (http://www.digitpa.gov.it/cad), addresses a set of ethical issues such as:

- the participation to administrative proceedings through information technologies ("Participation in the administrative procedure and the right of access to administrative documents can be exercised through the use of information technology and communication according to the provisions of Articles 59 and 60 of the Presidential Decree of 28 December 2000, n. 445");
- Democratic Electronic Participation ("Public administrations encourage any form of use of new technologies to promote greater participation of citizens, even living abroad, in the democratic process and to facilitate the exercise of political and civil rights both individual and collective")
- Privacy of data transmitted electronically ("Persons working with electronic transmission of documents, data and documents drawn up by computer cannot take cognizance of electronic correspondence, duplicate by any means or transfer to any third parties information about the existence of correspondence, communications or messages transmitted over the Internet and the related content and any part/extract of it, except in the case of information by their nature or by express indication of the sender intended to be made public")

2.4.4 Greece

Greek legislation regarding public participation, environmental issues, electronic communication, e-Government policies, and personal data protection are [15]:

- Common Ministerial Decision No. 77921/1440/1995 on the free access of the public to Authorities concerning environmental information.
- Greek Law 3242/2004 and Greek Law 3448/2006
  Self-imposed search of documents by the public authorities, use of information of the public sector: Direct communication among competent Authorities for issuing certain types of documents which might be needed for environmental authorization and environmental control should be requested by the Environmental Authority through direct communication with other competent Authorities.
- Greek Law 3861/2010 for administrative decisions' publication on the CL@RITY website.
  Cl@rity platform is an initiative of the Greek Ministry of the Interior, Decentralization and e-Government, aiming at the enhancement of transparency of all public administrations of National, regional or local level in Greece. All public entities, are obliged to upload all the decisions to the Cl@rity portal, and each decision or document is digitally signed and assigned a unique transaction number automatically. The whole process contributes progressively to a cultural change of the Public Administration and creates a more transparent relationship between the citizens and the State. Cl@rity initiatives state that there should be open and equal access for all citizens to the outcome of the Environmental Permitting Process, renewal or amendment of the Decision of the Environmental Approval [16].
- Greek Law 3852/2010, Articles 227 and 238.
  All citizens have the right to appeal against decisions of the Public Administration within a deadline, invoking the appropriate documentation or arguments.
- Greek Law 4042/2012, Article 55.
  (Governmental Gazette Vol. A/24 /13.02.2012) determines the penal protection of the environment (in compliance with the Directive 2008/99/EU – Frame of production and management of waste - Compliance with the Directive 2008/98/EU – Regulation of issues of the Ministry of Environment, Energy and Climate Change)."

Also Greek national framework provides two other laws that are very important for e-Government services and the privacy of personal data.

- Greek Law 3979/2011 concerning e- Government
  (Governmental Gazette Vol. A/ 138/16.06.2011) "On e-Government and other issues")
- Greek Law 2472/1997 concerning the protection of personal data.
  (Governmental Gazette Vol. A/50/10.04.1997). "Protection of the individual against processing of personal data")

2.5 Privacy Protection Issues in pilot scenarios

Privacy protection issues in the pilot countries have been identified by pilot partners and they have been considered according to the use cases of STEP platform and the issues that may arise. These are also reported as how these are addressed through legislation in each pilot country. Table 2 summarizes these issues as follows:

Table 2 Privacy Protection Issues that can raise in pilot scenarios

Transaction/Use case, stakeholders involved, data/information exchange	Issue that can arise	National and/or EU legislation addressing/regulating the issue
Submitting petition	Virus can affect the system & protection of submitted content regarding the petition	• Turkish Law No: 5651 – Regulating the internet transmission issues and combating the crimes which are conducted by internet transmission
E-government services in general	Accessibility and protection of submitted information	• Italian Law, Art. 4, 9 January 2004
Usage of personal data in electronic transaction (uploading documents, submitting forms with personal information etc.)	Protection of personal data, commercial confidentiality, protection of intellectual property	• Italian Legislative Decree 30 June 2003, 196 • Italian Legislative Decree 7 March 2005, n. 82
Administrative policy making and participation process, led electronically, affecting the public interest	Transparency issues, Democratic Electronic Participation	• Italian Law, 7 June 2000, n. 150 • Italian Legislative Decree 7 March 2005, n. 82
Electronic Data Usage (Uploading, exchanging documents, GIS data etc.)	Security of Information and Data (Personal Data, Administrative Data) Accessibility Rights to the Government Services electronically Administrative Procedures (Stakeholders Requests, Administrative Decisions, Submittals and Transmittals complying the Deadlines) Liabilities arises due Data Usage and Storage (Industrial and Intellectual Property Rights, Protection against Espionage)	• Article 4 and 6 of Turkish Law No 5809 – Law on Electronic Communication • Article 132,135, 136 and 137 of Turkish Penal Code No:5237: Personal Information Registry, Disclosure • Article 4 and 8 of Regulation on Personal Information Registry and Protection of Privacy (Directive (95/46/EC)) • Turkish Law on Civil Servants No:657 Turkish Law on Competition No:4054 Decree on Protection of Commercial Secrets and Access Rules to the Commercial Information No:2010/3 • Turkish Law on the Right to Access Information No:4982/2003
Personal and Sensitive Data Management	Misuse of personal and sensitive data	• ES: Organic* Law 15/1999, 13th of December focused on Personal Data Protection
Personal and Sensitive Data Management	Data usage for private/market purposes	• ES: Royal Decree 1720/2007, 21th of December, in which the regulation implementing the Organic Law on Protection of Personal Data was adopted
Hackers attacking the system	Privacy protection issues	• ES: Law 19/2013 , 9th of December, on Transparency, access to public information and good governance • CAT: Law 19/2014, 29th of December, on Transparency, access to public information and good governance • Royal Decree 3/2010, 8th of January, in which the National Security Scheme (ENS) is regulated in the field of eGovernment

3 Legal & Ethical Framework for Involvement of Human Subjects in the Testing

The overall objective of the STEP project is to develop and pilot test a cloud eParticipation SaaS platform, (available as a mobile application and through a web platform), whose goal is to engage Young European Citizens and Public Authorities in discussions about environmental policies. Within the remit of STEP, two main ethical questions arise:

- Will the people involved in the testing be exposed to any harm?
- Will the people involved in the testing represent all the social groups that will use the service?

According to Frankel and Siang (1999), "ethical and legal framework for protecting human subjects rests on the principles of autonomy, beneficence, and justice". Autonomy reflected in the process of informed consent, in which the risks and benefits of the research are disclosed to the subject. Beneficence and justice also tries to maximize the benefits of the research while minimizing the risks for subjects of a fair distribution to keep the balance among subjects [5].

ICT research may cause harm related to: systems assurance (confidentiality, availability, integrity); individual and organizational privacy; reputation, emotional well-being, or financial sensitivities; and infringement of legal rights (derived from constitution, contract, regulation, or common law) [6].

During the STEP pilot phase, in each pilot location, user groups will be involved in the testing of different segments of the solution according to their interest and local priorities. The feedback from the users will be collected, processed and analyzed for evaluation purposes. The STEP partners should:

- inform potential research subject on the research protocol, risks they could face (if there are any identified) and research benefits
- obtain consent from research subjects
- inform research subjects that they can withdraw from research at any time without suffering negative consequences
- ensure anonymous participation of research subjects
- ensure not to give harm for the testers of STEP platform
- provide necessary help and support to the interested research subjects

4 Impact of Cloud Computing On Privacy Protection

In a Cloud computing environment, private or commercially sensitive data may be stored, accessed and processed in remote locations, including for example different countries. Thus data protection and identity management become increasingly important to assure continued trust in and uptake of these services [7]. Governance models and processes need to take into account the specific issues arising from the inherently global nature of the cloud.

Altough the **European Digital Agenda**[6] promotes the development of an EU-wide strategy on cloud computing, the current legislation, both at European and at local level, does not explicitely address the cloud/software as a service environment.

This lack of a common and clear regulation, in terms of cloud-computing for e-Government services, leads to some uncertainity in the design of Cloud e-Government solutions. The requirements to be taken into consideration while designing an e-Government service on the cloud and when a key focus is the privacy protection, are those related to the management of data [13-14]. Data is subject to specific legislative requirements that may depend on the location where they are hosted or on the purposes for which they are processed. In the cloud case, there is a lack of clarity on applicable law, due to the cross-border situations where the data subject, the data, the controller, the processor and the processing may be located in different countries (Articles 25 and 26 of Directive 95/46/EC) [1].

Privacy protection is one of the main concerns to be taken into account in the design of eGovernment services to be deployed on the Cloud, as trust in Cloud computing is a key prerequisite. Different countries have different laws regarding which kind of data may be hosted in a cloud, where and how it is to be protected and may be accessed or made public. Within the cloud, technically data may be hosted anywhere within the distributed infrastructure, i.e. potentially anywhere in the world. National legal frameworks will guide platforms to work as eGovernment services on cloud.

Among the barriers for the adoption of the 'e-Governemet service on the Cloud' business model, moving sensitive corporate data to the Cloud is one of the most relevant to face from the user perspective, while the difficulties to achieve the required scale when different rules (e.g. regarding data location) have to be obeyed, is a key problem from the service provider point of view.

This is why, the recommendation drafted by the industry workgroup to the European Commission on the orientation of a Cloud computing strategy for Europe in terms of privacy is to 'Ensure privacy legislation is horizontally assessed for its compatibility with Cloud computing, and is looked at in a global context [8].

This recommendation translates into two specific actions for the European Commission:

1) *The EC should ensure the review of the Data Protection Directive delivers a result that facilitates Cloud computing in Europe and at a global level and consider the impact of the national implementations of the Data Protection and ePrivacy Directives on the Cloud.*

[6] https://ec.europa.eu/digital-agenda/en

2) *The EC should work with other jurisdictions/regions to develop interoperable requirements that facilitate information flows with appropriate security and privacy protection, including the opportunity to build upon recognised existing global initiatives.*

As it is not possible to wait that the EC takes the required legislative action to start the implementation of the STEP platform, the impact of the cloud computing environment on the data protection issues have to be minimized, applying, if necessary, restrictive policies.

STEP platform controller (acting in this case as 'cloud client') is required to define a service contract with the cloud provider defining the responsibilities of each party in the management of data protection in accordance with the current legislation. This contract must at a minimum establish the fact, that the processor has to follow the instructions of the controller and that the processor must implement technical and organizational measures to adequately protect personal data.

To ensure legal certainty the contract should also set forth the following issues:

- Specification of security measures that the cloud provider must comply with, depending on the risks represented by the processing and the nature of the data to be protected.
- Subject and time frame of the cloud service to be provided by the cloud provider, extent, manner and purpose of the processing of personal data by the cloud provider as well as the types of personal data processed.
- Specification of the conditions for returning the (personal) data or destroying the data once the service is concluded. Furthermore, it must be ensured that personal data are erased securely at the request of the cloud client.
- Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to data.
- Obligation on the provider's part to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data.
- The contract should expressly establish that the cloud provider may not communicate the data to third parties, even for preservation purposes unless it is provided for in the contract that there will be subcontractors.
- Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data.
- Obligation of the cloud provider to provide a list of locations in which the data may be processed.
- The controller's rights to monitor and the cloud provider's corresponding obligations to cooperate.
- It should be contractually fixed that the cloud provider must inform the client about relevant changes concerning the respective cloud service such as the implementation of additional functions.

- The contract should provide for logging and auditing of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors.
- Notification of cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited.
- A general obligation on the provider's part to give assurance that its internal organization and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards.

In addition, in order to overcome the problem of different laws that apply to the same data, the cloud provider may be required to equip the hosting of the STEP service entirely within an EU country in which it is delivered, and to ensure that the data does not go beyond the boundaries. If a non-EU country asks for the STEP service to be ensured that data does not go beyond their boundaries and hosted in their region, the cloud provider may be required to host a specific instance in that country for only local environmental issues.

5 Environment Protection

STEP is a platform that aims to promote the societal and political participation of young people in the decision-making process on environmental issues. Therefore environment protection is an important aspect to be considered from an ethical perspective. General ethical framework related to the environment is shaped in the Convention on access to information, public participation in decision-making and access to justice in Environmental Matters (Aarhus Convention) signed in 1998 and ratified by most of the European countries and the European Union (decision 2005/370/EC). STEP **Deliverable 2.1 "Report on decision making procedures"** presented related conventions and regulatory framework for public participation in environmental issues, here we foucs only on key selected aspects.

As an international instrument for the protection of the environment this Convention contains three groups of principles relating to:

- The right of citizens to access to information;
  "Any environmental information held by a public authority must be provided when requested by a member of the public, unless it can be shown to fall within a finite list of exempt categories" [9]
- The right of citizens to participate in decisions about the environment;
  "The Convention sets out minimum requirements for public participation in various categories of environmental decision-making" [9]
- The right to access justice when the previous two rights are violated.
  "The third pillar of the Convention (article 9) aims to provide access to justice in three contexts:
  - review procedures with respect to information requests
  - review procedures with respect to specific (project-type) decisions which are subject to public participation requirements, and challenges to breaches of environmental law in general.

Thus the inclusion of an 'access to justice' pillar not only underpins the first two pillars; It also points the way to empowering citizens and NGOs to assist in the enforcement of the law [9].

A directive on public Access to environmental information has been accepted by European Parliament within 2003/4/ES Directive. This directive regulates the rules that ensure free access to and dissemination of environmental information held by public authorities and defines the basic terms and conditions under which such information should be made available. It also defines the term "environmental information":

"Information in relation to the environment means any written information available visual, audio, electronic or any other form of state of water, air, soil, fauna, flora, land and natural areas, as well as measures or activities that affect the environment or that are designed for their protection."

The Directive aims to guarantee that environmental information is systematically available and disseminated to the public.

6 STEP Platform Ethics Guidelines

Privacy and data protection are socio-technical issues relevant for software development projects and system design. They lead to requirements for the design of the technical infrastructure as well as for policies and agreements that have to be enforced on an organizational level. Data privacy is the right of any individual to expect that his/her personal information directly or indirectly collected are processed securely and are not disseminated without their written consent. Data privacy must not be subject to "mission creep" i.e. information collected with permission for one purpose and used without permission for other reasons. Data protection is the framework of security measures designed to guarantee that data are handled in such a manner as to ensure that they are safe from unintended, unwanted or malevolent use. Data protection is the technical mechanism to ensure data privacy.

In Horizon 2020, considering ethics issues arise in many areas of research such as the medical field, research protocols in social sciences, ethnography, psychology, environmental studies, security research, etc. and these research and innovation projects might involve the voluntary participation of research subjects and the collection of data that might be considered as personal; a guideline for ethical & legal issues has been provided for self-assessment of proposals [10].

A crucial aspect to be considered in this context is the wide scale deployment of cloud computing services, which can trigger a number of data protection risks, mainly a reduced control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed/sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider.

The lawfulness of the processing of personal data in the cloud depends on the adherence to basic principles of the EU data protection law, on the basis of which it's possible to define the following recommendations for the STEP platform in relation to data protection:

Minimization: STEP platform should only handle minimal data about users.

Transparency: the STEP platform should inform data subjects about which data will be stored, who these data will be transmitted to and for which purpose, and about the cloud provider and all subcontractors (if any), as well as about locations in which data may be stored or processed by the cloud provider and/or its subcontractors.

Consent: Consents have to be handled through the user interface allowing the users to agree the transmission and storage of sensitive data. The consent text included in the interface should specify which data will be stored, who they will be transmitted to and for which purpose for the sake of transparency. An applicant, who does not provide this consent for data necessary for the participation process, will not be allowed to participate the platform. The consent legal text must be customized for each pilot country with references to the local legislation that applies.

Defaults: By default data is not automatically shared. Data sharing and diffusion applies just to data for which consent has been given, and in accordance with the diffusion terms expressed by the consent.

Purpose specification and limitation: personal data must be collected just for the specified purposes of the participation process and not further processed in a way incompatible with those purposes. So not only the authority offering the service must guarantee that personal data are not processes for purposes not

compatible with the original ones, but it must be ensured that personal data are not (illegally) processed for further purposes by the cloud provider or one of his subcontractors. So the applicant and other involved stakeholders, when they register into the system, have to receive a legal note specifying this.

Erasure of data: personal data must be kept in a form that permits the 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. Personal data that are not necessary any more must be erased or truly anonymized. If this data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be blocked. The cloud client should make sure that the cloud provider ensures secure erasure and that the contract between the provider and the client contains clear provision for the erasure of personal data. The same holds true for contracts between cloud providers and subcontractors.

Anonymity: The anonymous participation of citizens to the proceeding shall be enabled for those countries whose legislation explicitly defines this right.

Accountability: it shall be possible to establish what an entity did at a certain point in time in the past and how.

Cookies: The system shall not store cookies on the users' computers to prevent any unauthorized tracking of the users' activities on the Internet.

Security: The protocol used for data exchange within STEP shall support encryption with SSL and TLS, which can be regarded as state-of-the-art encryption methods. Encryption of personal data should be used in all cases when "in transit" and when available to data "at rest". STEP platform, as relying on the encryption solution offered by the cloud provider can be considered a risk, shall evaluate the encryption of personal data prior to ending them to the cloud. Communications between cloud provider and client as well as between data centers should be encrypted. Remote administration of the cloud platform should only take place via a secure communication channel.

Hosting of Data: it shall be evaluated to require the cloud provider to equip the hosting of the STEP service entirely within each single country in which STEP is delivered and to ensure that the data does not go beyond the boundaries of that country.

The following section provides guidelines and the technical approach taken for the relevant ethical issues including human involvement, personal data protection, third countries and environment in STEP platform.

6.1 STEP Technical Approach

The technical solution set-up for the STEP Platform has taken into due consideration the recommendations drafted in this document and these will be implemented in order to minimize its impact in terms of privacy and confidentiality of personal data. This section of the deliverable illustrates the technical choices made with respect to these issues. Some additional development is envisaged before the operational launch of the platform, in order to fully accomplish the recommendations defined in this document.

STEP has been built on components based on different technologies including Microsoft ASP.Net, Java, HTML5, Javascript, etc. These have been presented in the project Deliverable 2.2. The eParticipation platform component is based on ASP.Net MVC framework and uses Entity Framework, Signal R, MassTransit, RabbitMQ, JQuery and several other small libraries. The social media mining component is based on Java, and uses mongoDB for storing data collected from social media APIs, and data produced by analyzing the collected data. The visualization component is implemented using HTML5/CSS3 for the layout of widgets, and JavaScript for handling dynamic data loading and the visualizations. In particular, the D3.js library is used as a basis for the visualizations. Machine Translation component is using a web server based framework, Ruby on Rails (RoR) for the front end and uses Java Technologies with MySQL database and Moses framework. Data logging component is based on Microsoft ASP.Net MVC framework, uses ASP.Net WebAPI as the eParticipation platform, Windows Communication Foundation (WCF) and Entity Frameworks respectively.

The STEP platform uses a number of security policies and rules to ensure the confidentiality, integrity and availability of electronic information captured, stored, maintained, and used. STEP e-Participation provides authentication mechanisms and policies to assure authorized access to the platform's data, the generation, maintenance and transmission of strong passwords. The platform provides User Access Control mechanisms that provide the right privileges to the platform users. The platform also provides additional security mechanisms in order to protect data and eliminate risks such as SQL injection, Cross-site scripting (XSS) and session hijacking. Furthermore, the platform supports secure protocols (SSL) and encryption mechanisms to allow the secure transmission of sensitive information over the network.

The STEP platform is hosted on a secure data center infrastructure, which is controlled by the coordinator, DRAXIS and is designed considering the cloud computing recommendations and technical requirements in D2.2 User & Technical Requirements deliverable. It provides an extremely scalable, highly reliable platform that enables users to deploy applications and data quickly and securely.

6.1.1 Protection of Personal Data

The project raises some ethical issues that the consortium is aware of and will take appropriate measures to cover them. In particular, the pilot implementation and the utilisation of the STEP Platform from the end users perspective requires the collection and storage of private and sensitive data. Thus, one of the main concerns during the development of the project will be the protection and handling of these data. The consortium guarantees that all personal data collected during the project will be kept secure and unreachable by unauthorized persons. The data will be handled with appropriate confidentiality and technical security, as required by law in the individual countries and EU laws and recommendations. It should be noted that all the government organizations that participate in the consortium have in place their own data privacy and security policies which are compliant with EU regulations.

All activities will be carried out ensuring the ethical principles in accordance with Directive 95/46/EC of the European Parliament, about the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as DIRECTIVE 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, as

modified by Directive 2009/136/EC. All national data protection and privacy laws for pilot countries will be also followed.

Moreover, the protection of personal data will also be ensured through procedures and appropriate technologies, like the use of HTTPS protocol for the encryption of all internet transactions and appropriate European and Internet security standards from ISO, ITU, W3C, IETF and ETSI. Protection of personal data is ensured by the use of Open Source solutions and architecture. The STEP platform will be based on both open source and proprietary based frameworks like Microsoft .NET and standards which are publicly available and their security levels can be easily tested.

To assure the participants privacy, all data will be anonymised, encrypted and stored on a server to which only the relevant staff have access. More specifically the server onto which the data will be stored will have server side encryption. That means that the server's administration personnel will be able to generate public keys for specific personnel who will have access to the data but will not be able to access the data themselves (since the private keys required for this access will be generated on the machine of the person with access to the data). That means that only the required personnel will have access to the data and even in the remote case of a possible data leak or server hack the data stolen will be fully encrypted and thus fully non accessible. Based on anonymized data, some statistics will be provided as open data for research purposes according to D1.3 STEP Data Management Plan.

In the case of social media content, no encryption takes place since there is significant computational overhead in encrypting large amounts of dynamic data, which makes it impractical for social media content. However, the data is stored on a secure server with access possible only to personnel working on the development of the component.

6.1.2 Personalized service and anonymous aggregation of user choices

Personalised services will be offered on the basis of registered user profiles that will be stored in the application server, deployed at a data center controlled by the coordinator, and accessible only by authorized personnel. No passwords will be stored (only hashes) and therefore the personal profile information (including name, email, preferred topics and voting history) will be only accessible by the registered user. User registration, authentication and data access will be implemented according to state of the art security practices and standards. In addition, the anonymous aggregation of user choices and social media content will be used to derive trending topics, content, influencers and other aggregate insights. This aggregate output will be matched and presented to each registered user in a personalised way, by means of filtering based on his/her profile and personal interests that he/she will have designated in his/her private profile, which will be stored on a secure server and will be accessible via secure authentication methods, as described above.

The aim of the user interaction log system is to understand the usage of different parts of the software component and user interface (UI) elements and update the front end based on the usage patterns, which is not directly linked with personalised content, profile and preferences. User choice and interface

accessing will be based on anonymously classified and logged data (age, gender, etc.) which is not related with the personalised profile or preference of the user. This anonymous aggregated data gives an accurate log of how users actually use the system. Anonymous aggregation of user choices and interface accessing will let the consortium know about the usage of the platform and is not providing a conflict with the personalised information provided.

6.1.3 Ethics Approval

Copies of ethical approvals for the collection of personal data or the respective notifications (depending on the type of personal data that will be collected and according to the national data protection legislation of each country) by National Data Protection authorities or Ethics Commitee will be submitted to the Research Executive Agency (REA)[7].

6.1.4 Collection and/or processing of personal data for research purposes

The project performs and will perform user studies and tests during its research and evaluation stages. For the conduction of the user studies no personal sensitive data will be required. Following the best practice for ethics in Human-Computer Interaction [17], any personal (but not sensitive) data collected during the user evaluations will be anonymized or at least pseudonymized and used for the purposes of the project. The data may include personal information about the user such as: first name, surname, e-mail address, phone number, postal address, date of birth, interests, posts, likes, comments, location, images, or relations to other users. They will not include sensitive personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction). The participation is voluntary and informed consent is collected from each individual user. In addition, an Information Sheet is provided to each contacted individual, i infoming them about the the scope of the research and where additional information can be sought.

Following the guidelines, in the requirements gathering (D2.2) phase, informed consent was obtained from participants participating to qualitative interviews. These participants were also provided with an Information Sheet presenting the project, its goals and purposes. The same process will be used for other stages of user research/evaluation and in particular for the work related with D4.1 (with the conduction of a cultural probe) and D5.3 (with the conduction of evaluation via questionnaire and usability testing) The requirements data collected is being used to inform the design of the platform and for use in research publications including project deliverables. This collected data is stored Securely on the Abertay University Research Data Storage Drive and any identifiable data is encrypted prior to storage. Access to this data is restricted to the researchers involved in the Project considering the data protection guidelines in this document. This data is additonally protected in accordance with the University's legal requirements under the UK Data Protection Act and in accordance with the Research Code of Conduct & Data Management Policies of the University the data will be stored for a period of 10 years. This

[7] http://ec.europa.eu/rea/index_en.htm

requirements data is stored and then destroyed in accordance with Abertay's Data Management Policy.[8] The subjects are offered the contact details of the research team and they are informed about protection and data altering mechanisms at the time of data collection. Data is collected only with users' explicit knowledge and no raw data is publicly available. This data is only accessible for research purposes by project partners under the rules of the consortium agreement, ethics guidelines and specific research policies.

6.1.5 Procedures for data collection, storage, protection, retention and destruction

The general framework by which data collection, storage, protection, retention and destruction is performed according to EU legislation, directives and opinions is laid out in details in Section 6.1. Below we present specific policies that implement the privacy recommendations in sections 6.1.1, 6.1.2, 6.1.3 and 6.1.4 in the project mobile application and website. Each partner will comply with their national and EU data protection law, including notification of their national Data Protection Authority if necessary under their national law, when processing the personal data of the project applications users or any other personal data processed in the context of the project.

Each partner will provide precise information on what type of personal data they process concerning the project applications users, how it is processed and which data-flows they enable. Each partner will also provide an email address to be contacted in case a user wants to withdraw his/her consent for processing his/her personal data; this is preferably the same email address as the one used to gain further information, but will be available through the STEP website.

All parties shall carry out a personal information assurance risk assessment from their own context concerning their own collection, storage and/or processing of personal data, prior to deployment of the live service when personal data will be collected, and at any point through the operation of the system where there is a relevant change to either hardware installation, software versions, and/or software interfaces. Such a risk assessment shall follow information assurance principles covering, at least, hardware installation, software development processes, software validation and approval, software execution and backup processes. Each partner is liable for inappropriate security at its own premises.

For data collection purposes, the official APIs that are made publicly available from the respective online sources will be used, and always in full compliance with their terms of service.

In terms of data retention and destruction, data will be deleted or fully anonymized as soon as the relevant scientific purpose as stated in the DoW is fulfilled.

Regarding data processing, the collected data will be immediately pseudonymized and aggregated, and the original data will not be stored whatsoever.

[8] https://intranet.abertay.ac.uk/media/Management%20of%20Research%20Data%20Policy%20and%20Guidelines.pdf

With respect to data storage, personal data of the users of the application will be stored in secure servers in the control of DRAXIS, after first having notified the Greek Data Protection Authority accordingly. Appropriate technical measures will be taken for secure data access and user authentication.

6.1.6 Web and social media mining and monitoring tools

The web and social media mining and monitoring tools to be deployed in the project will collect and/or process publicly available personal data, abiding to all relevant rules and recommendations of the national legislation and the respective EU recommendations and directives. For data collection, the official APIs that are made publicly available from the respective online sources will be used, and always in full compliance with their terms of service. Social media posts and basic profile information from the users social media account is collected based on keywords and data from social media are processed and aggregated to create data summaries. Furthermore, some individual items are shown to the user interface of the visualization component. All data collected from social media are stored in a mongoDB installation in the STEP servers. No cross-referencing takes place in the social media mining component. The data is stored in the form they are collected from the respective APIs. No further accuracy assurance is performed. Subjects will not be able to alter information as this is already published information that is collected from third party services. The collected social media data may be disclosed to researchers working only on the project and to pilot partners testing the system based on the guidelines and consortium agreement.

6.1.7 Non-EU countries

We confirm that the ethical standards and guidelines of Horizon2020 will be rigorously applied, regardless of the country in which the research is carried out. For data transfer to non-EU countries, we will make a data transfer agreement with the recipient and obtain a specific authorization by the national data protection authority for data transfer to third country (if required).

6.1.8 Right to be forgotten and to erasure

Pilot users will have the right to obtain the erasure of personal data relating to them and the abstention from further dissemination of such data according to the General Data Protection Regulation [11]. They will be informed about this right in the information sheets. Applications for erasure of data will be carried out without delay. In case the personal data has been made public, the consortium will take all reasonable steps, including technical measures, to inform third parties that are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. A procedure for exercising the right to be forgotten and to erasure will be provided, and will include appointment of a data protection manager, checking the validity of the request, identifying data which should be erased, monitoring the erasure process, and informing the pilot user.

Need to know principle Data collected and processed will be anonymized, encrypted and stored on a server which will have server side encryption. This means that the server's administration personnel will be able to generate public keys for specific personnel who will have access to the data but will not be able to access the data themselves (since the private keys required for this access will be generated on the machine of the person with access to the data). This means that only the required personnel (specifically assigned by the project partners) will have access to the data.

7 Conclusion

D2.3 Guidelines for handling ethical, legal issues and data protection has detailed EU level and national frameworks for handling ethical, legal and data protection issues. This deliverable aimed to identify key issues that can arise throughout the life of the STEP project, considering aspects specific in each pilot country (Turkey, Greece, Spain, Italy) and generally valid at the EU level.
In Horizon 2020 research and innovation projects, ethical issues may arise on aspects such as involving human embryonic stem cells (hESCs), human embryos or fetuses, involving work with humans, using, producing or collecting human cells or tissues, collecting and processing of personal data, involving animals, third countries, environment protection, dual use, misuse of research data and other ethics issues that may not be listed in Ethics Issue Table in the Horizon 2020 guidelines.

This deliverable first investigated corresponding European directives including Data Protection Directive, e-Privacy Directive and Cookie Directive with the support of all national frameworks of pilot countries (Turkey, Italy, Spain and Greece). Ethics issues based on scenarios have been presented and solutions on how to address them have been provided, considering human subjects' involvement, cloud computing impact and environment protection issues. Regarding the issues and regulatory frameworks analyzed, guidelines and the technical approach for the STEP platform are provided for the use of all partners and other Work Packages. Guidelines and the STEP technical approach include solutions for the collection, processing and protection of personal data, personalized service and anonymous aggregation of user choices, ethics approval, procedures for data collection, storage, protection and retention of data, specific ethics analysis for social media mining and monitoring component and non-EU countries involvement.

The research conducted in this deliverable includes several important aspects of privacy & data protection from EU and national regulatory framework and technical perspectives. The ethical analysis of cloud based e-Government applications and participation will be of interest for all work packages of STEP project.

The guidelines in the deliverable will be a reference for technical and pilot partners of the STEP platform both during the implementation and execution phase, and also for the exploitation of the platform which the consortium expect the deliverable to reach a wider audience of policy makers and researchers for further projects.

8 References

[1] Directive 95/46/EC of 24 October 1995 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 31-50.

[2] Directive 2002/58/EC of 12 July 2002 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal. L 201, 31/7/2002 p. 37-47.

[3] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF)

[4] Almarabeh, Tamara and AbuAli, Amer (2010). A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success. European Journal of Scientific Research, vol. 39(1), pp. 29-42

[5] Frankel, M.S. & Siang, Sanyin (1999). Ethical and legal aspects of human subjects research on the Internet. Report, American Association for the Advancement of Science

[6] The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, D. Dittrich and E. Kenneally, eds., US Dept. Homeland Security, 2011; www.cyber.st.dhs.gov/wp-content/uploads/ 2011/12MenloPrinciplesCORE-20110915-r560.pdf .

[7] eEnviPer Newsletter #2, eEnviPer Consortium, May 2013, http://eenviper.eu/uploads/files/1305_eEnviPer_Newsletter_2.1.pdf.

[8] Unleashing the Potential of Cloud Computing in Europe, 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[9] UNECE Environmental Policy, Access to Information, http://www.unece.org/env/pp/contentai.html

[10] Horizon 2020 How to complete your ethics Self-Assessment, 2014

[11] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Parliament.

[12] Charter of Fundamental Rights of the European Union (2000/C 364/01, http://www.europarl.europa.eu/charter/pdf/text_en.pdf)

[13] Cloud computing: indications for the conscious use of services, Italian Guarantor for the Protection of Personal Data, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1819951, 23-06-2011

[14] CLOUD COMPUTING: HOW TO PROTECT YOUR DATA WITHOUT FALLING FROM A CLOUD, Italian

Guarantor for the Protection of Personal Data, http://www.garanteprivacy.it/documents/10160/2052659/1912744, 24-05-2012

[15] Arkouli, K.G. (2011). The legal framework of personal data e-processing in the digital environment in Greece. Fourth International Conference on Information Law and Ethics, Thessaloniki, 20-21 May 2011.

[16] CL@RITY website, Terms of use–Policy of personal data protection. http://www.diavgeia.gov.gr

[17] Minocha, Shailey and Tzanidou, Ekaterini (2010). Ethics in usability engineering. In: India HCI 2010/Interaction Design for International Development, 20-24 March 2010, Industrial Design Centre, Indian Institute of Technology, Bombay, Mumbai, India.

9 Appendix:

9.1 Data Protection Checklist

Hereafter is reported a privacy checklist and questionnaire, which can be seen as a general tool to ease the identification of the privacy issues that may impact a process, and have to be considered in the operational implementation of the process itself and in the set-up of the IT tools that support it.

In relationship with the use cases designed for the STEP platform and the consequent pilot execution, the following points have been considered:

- Who can collect information?
- Under what circumstances is information within a specific category collected?
- With whose consent is information within a specific category collected?
- How is each type of data being used?
- How is each type of information stored?
- Are there different storage strategies in place for different classes of data?
- How is it cross-referenced?
- What uses are permitted with respect to each class of information?
- How long is each class of information retained?
- When is information belonging to each class destroyed, and who is accountable for its destruction?
- How is the accuracy of collected information assured?
- What access mechanisms are/will be in place, allowing the subject to alter/update inaccurate or obsolete information?
- To whom, under what circumstances, and in what manner may information belonging to each class be disclosed?
- What information is collected without a user's explicit knowledge and/or consent?
- What, if any, communications will occur between the website and the user?
- What method(s) of communication will be used (E-mail, Postal mail, Telephone call, Fax, Other)
- How frequently will the communication take place?
- Under what circumstances will such communications take place?
- Do the web platform and/or the organization share, transfer, or release any information to third parties?
- Does the web platform contain links to other websites?
- Is the information received directly from a user complemented with additional information received from third parties, or information received by mechanisms other than those to which the user has explicitly consented?
- Is access to personally identifiable and/or sensitive data accountable to specific individuals to maintain control over access and preserve accountability for misuse?

- Is access to data granted to parties outside of your organization? (Incl. Business partners, subsidiaries, etc.)
- Are certain groups or individuals granted general access to data within your organization?
- How do you verify the identity of the persons/parties accessing the data?
- Which measures are taken to ensure password security?
- Are there additional authentication requirements instead of, or in addition to, password security for access (biometrics, etc.)?
- What mechanisms are in place to ensure security/confidentiality of customer/user information during transmission over public communication lines and within the organization?
- Is sensitive information differentiated from less sensitive information, and is there any access restriction applied according to this categorization?
- Have Non-Disclosure/Confidentiality Agreements been executed with contractors and third parties, restricting/controlling access to/use of sensitive data?
- Is access to data limited to authorized personnel only? If so, which person(s) are authorized to access specific classes of information?
- Is access to sensitive data revoked in a timely manner from employees that change job functions or leave the organization?
- If third-party agreements exist to allow access to data, what mechanisms have been implemented to notify the responsible official (i.e., the Security Administrator) when the agreement is modified or terminated?
- What restrictions are in place to control merging of sensitive data with unprotected data?
- Is there a mechanism in place to allow users' access to their information in order to verify that the data is accurate and has not been modified or corrupted?

9.1.1 Data Protection Main Questions

The STEP project also applied the self-questionnaire below to examine the data privacy and protection issues in a structural manner. This guideline is used as a Data Protection Checklist by the Data Protection Commissioner of Ireland and is also used here as a supporting tool[9].

Fair obtaining:

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them
- Can we describe our data-collection practices as open, transparent and up-front?

Purpose specification

[9] https://www.dataprotection.ie/docs/Self-Assessment-Data-Protection-Checklist/22.htm

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with the Data Protection Commissioner, does our register entry include a proper, comprehensive statement of our purpose? [Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Use and disclosure of information

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.
- If we are required to register with the Data Protection Commissioner, does our register entry include a full list of persons to whom we may need to disclose personal data? [Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.]

Security

- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?
- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorized people?

Adequate, relevant and not excessive

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?
- Does a policy exist in this regard?

Accurate and up-to-date

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Retention time

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the Act's requirements?

Registration

- Are we clear about whether or not we need to be registered with the Data Protection Commissioner?
- If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? [Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]
- Is a named individual responsible for meeting our registration requirements?