COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT PSP call for proposals 2011

Project Acronym: **eEnviPer**

Project Number: **297358**

Project Type: **Pilot Type B**

Project Full Title: **A single multi-purpose SOA platform that delivers environmental permissions services through the cloud of e-Government services and applications**

ICT PSP Main Theme addressed: **4.1 - Towards a cloud of public services**

D6.3 Privacy Impact Assessment Report

Nature:	**Report**
Dissemination Level:	**Confidential**
Version #:	**1.9**
Delivery Date:	**31 March 2014 (M24)**
Deliverable Leader:	**Planetek**
Author(s):	**Diomede Illuzzi, ALL PARTNERS**
Status:	**Final**
Reviewed on	**30.03.2014**
Reviewed by:	**SAMPAS**

Abstract

This deliverable provides the analysis about the privacy and data protection issues to take into consideration as inputs for design of the technological solution, and for the definition of the pilot execution strategy of eEnviPer in every pilot country and post-project exploitation.

The document was produced in two subsequent iterations with contributions, coming from all the project partners, gathered through two questionnaires.

A preliminary draft version of the document was released internally in November 2012, before that the technical implementation of the system started, in order to provide key guidance to the technical design of the overall solution (WP3) and the design of the pilot protocols (WP4). The first questionnaire was produced, therefore, with the purpose to assess the local legal frameworks, classify information managed in the designed workflows according to privacy levels, and Identify consequentially potential privacy issues in eEnviPer platform.

A second questionnaire, then, was distributed among partners in order to collect information about any privacy issues affecting the pilot execution and, furthermore, indication about best practices in place in the different pilot countries, in terms of privacy and data protection.

This contributions are reported in the final version of the document that, moreover, describes how the eEnviPer technical solution faces the privacy and data protection issue.

Document History

Version	Issue Date	Stage	Content and changes
#0.1	26 October 2012	Draft	Legal framework for privacy protection
#0.2	9 November 2012	Draft	Inclusion of contributions coming from all partners with description of privacy protection issues in the system data flows
#1.0	28 November 2012	Draft	First draft internally released, with guidance and recommendations for the system implementation
#1.1	29 April 2013	Draft	Addition of chapter *2.1.4 : Electronic Signatures*
#1.2	28 June 2013	Draft	Addition of chapter *6 : The eEnviPer Technical A*
#1.3	29 November 2013	Draft	Addition of chapter ***Error! Reference source not found.*** *:* ***Error! Reference source not found.***
#1.4	31 January 2014	Draft	Completion of chapter ***Error! Reference source not found.*** *:* ***Error! Reference source not found.*** with requirements for location of data managed by the service and addition of ***Error! Reference source not found.***
#1.5	14 February 2014	Draft	Review of chapter *7:* ***Error! Reference source not found.***
#1.6	26 March 2014	Draft	General review and inclusion of chapter *8 Conclusion.*
#1.7	26 March 2014	Draft	Review of chapter *6 : The eEnviPer Technical A*
#1.9	30 March 2014	Final	Final Review by SAMPAS

List of participants:

No	Partner	Acronym	Country
1	DRAXIS ENVIRONMENTAL S.A.	DRAXIS	Greece
2	KRITI	CRETE	Greece
3	ARISTOTELIO PANEPISTIMIO THESSALONIKIS	AUTH	Greece
4	PLANETEK ITALIA SRL	Planetek	Italy
5	AGENZIA REGIONALE PER LA PROTEZIONE AMBIENTALE	Arpa Puglia	Italy
6	STELLA Consulting SPRL	STELLA	Belgium
7	Evrogeomatika d.o.o.	EGEO	Serbia
8	Municipality of Indjija	Indjija	Serbia
9	NIGDE BELEDIYESI	NIGDE	Turkey
10	Sampas Bilisim Ve Iletisim Sistemleri Sanayi Ve Ticaret A.S.	SAM	Turkey
11	OIKON DOO ZA PRIMIJENJENU EKOLOGIJU	Oikon	Croatia
12	Krapinsko-zagorska zupanija	KZZ	Croatia
13	Province Directorate of Environment and Urbanism of Nigde	NCEDTR	Turkey

Table of contents

Executive Summary

The principal aim of the eEnviPer project is to provide an integrated web-based single multi-purpose cloud platform based on Service Oriented Architecture (SOA) to support environment-related permit procedures. The platform has been implemented and tested in five different European countries, namely Greece, Italy, Serbia, Croatia and Turkey.

The present deliverable focuses on the evaluation of the eEnviPer solution in terms of its impact on privacy of personal data throughout the life of the project.

Environmental permission is a transparent process that involves processing of personal data in a limited measure. The only "identifiable natural persons" in the process are: the investor or its legal representative, the Public Authorities officials and any consultant involved in the EIA evaluation. Also, we have to consider that a considerable percentage of the data involved in the EIA process will be made publicly available in order to guarantee the effective participation of citizens.

However, it is not possible to ignore the aspects of privacy when you want to set up an IT system, especially in the case of a Cloud solution, with the additional risks in terms of data protection that it involves.

This privacy impact assessment takes a structured approach, starting from the legislative framework, both at European and at national level, and analyzing, then, use cases both within the pilot terms and in the post-project deployment state.

Special attention is paid to the cloud computing environment in which the system will be deployed.

A first version of this document, which includes a set of recommendations based on the results of this analysis, has been produced and delivered internally – in November 2012 -, in order to provide key guidance to the technical design (WP3) and the design of the pilot protocols (WP4).

The final version of this document completes this analysis, reporting all the findings collected by the project partners in the context of the pilot executions, and illustrating how eEnviPer handled the privacy issues.

1 Introduction

This document is aimed to identify any issue that can arise in terms of privacy of personal data throughout the life of the project, considering aspects specific in each partner country and generally valid at the EU level.

Under the European Union (EU) law, personal data is defined as "any information relating to an identified or identifiable natural person". 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)
- Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)
- Directive 2009/136/EC (Cookie Directive)

Directives generally do not directly apply in the EU countries and need to be nationally implemented by each country through laws and regulations. As countries have some freedom in their implementation, stricter requirements than those prescribed by the directives may apply in certain EU countries. Furthermore, the data protection legislation is, in many respects, complemented or overlapped by sector specific legislation that also needs to be considered.

In order to get a clear, comprehensive and correct picture of the local data protection requirements, it is essential to check the national data protection laws, unfair competition legislation, telecommunications laws and any other local data protection regulations.

This privacy impact assessment takes a structured approach, analysing use cases both within the pilot terms and in the post-project deployment state.

The use cases in general consist of transactions between different stakeholders involved in the environmental permit issuing process (G2B, G2C, B2G, C2G …) which imply transfer / exchange of data / information. Any action that takes place in such e-Government service environment can potentially raise a privacy issue, addressed not only through technology but also through the procedures in place.

Privacy issues have to be considered, also, when the system comes to the testing and pilot execution phase, because collection of information about individuals, public entities and private organisations is necessary.

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).

That's why in some cases sometimes the cloud might not be considered the right fit. So we need to know if, at local level, a regulatory or security issue prevents us from hosting even encrypted data in a public cloud.

2 Legal Framework for Privacy Protection

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 "mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one of more factors specific to his physical, physiological, mental, economic, cultural or social identity".

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 legislature, that address and regulate the issue, starting from the "Charter of Fundamental rights of the EU" ([1]), which defines the fundamental rights of EU citizens, also in relationship to the privacy aspects. The Charter states that:

- "everyone has the right to respect for his or her private and family life, home and communications" (Article 7)
- "everyone has the right to the protection of personal data concerning him or her" (Article 8)
- 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".

The following paragraphs describe the most relevant laws and articles developing the subject of right to privacy.

2.1.1 Data Protection Directive

The Directive 95/46/EC (Data protection Directive, [2]) regulates the processing of personal data regardless 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) states that 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 the criteria for making personal data processing legitimate: personal data can be processed when one of the following conditions occurs:

(a) the data subject has given his consent

(b) processing is necessary for the performance of or the entering into a contract the data subject is party

(c) processing is necessary for compliance with a legal obligation the controller is subject

(d) processing is necessary in order to protect the vital interests of the data subject

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

(f) 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.

2.1.2 e-Privacy Directive

The provisions of directive 2002/58/EC on privacy and electronic communications (also known as e-Privacy Directive [3]) particularise and complement Directive 95/46/EC; contrary to Data Protection Directive, which specifically addresses only individuals, the E-Privacy Directive (Article 1(2)) also applies to legal persons.

This Directive is concerning 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.

The Directive is addressed both to the providers of electronic communications services (Article 4) - which are obliged to inform the subscribers whenever there is a particular risk - and to the Member States, who should prohibit listening, tapping, storing or other kinds of interception or surveillance of communications and “related traffic”, unless the users have given their consent, or a restriction of the scope of these rights and obligations constitutes a measure to safeguard national security.

This Directive is amended by Directive 2009/136/EC of the European Parliament and of the Council [5], which gives further requirements to the processing of personal data and the protection of privacy in the electronic communications sectors.

Below the text of the two most relevant articles are reported.

Article 4: Security of Processing

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational 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.

Directive 2009/136/EC of the European Parliament and of the Council [5] further specifies that the measures referred to in paragraph 1, shall:

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

Article 5: Confidentiality of the communications

1. 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 authorised 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.

2. Paragraph 1 shall not affect any legally authorised 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.

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

The e-Privacy Directive has been amended by the **Data Retention Directive** ([4]), in relationship to Telecommunications data retention. According to the directive, member states will have to store citizens' telecommunications data for six to 24 months stipulating

a maximum time period. Under the directive the police and security agencies will be able to request access to details such as IP address and time of use of every email, phone call and text message sent or received. A permission to access the information will be granted only by a court.

2.1.3 Cookie Directive

The EU Directive 2009/136/EC of the European Parliament and of the Council (Cookie Directive [5]) is an amendment of the Directive 2002/58/EC, which concerns the protection of data and privacy on the web.

The EU Cookie Directive requires websites to obtain informed consent from visitors before they store information on a computer or any web connected device. This is storage is mostly done by cookies, which can then be used for tracking visitors to a site.

Cookies, in fact, are hidden information exchanged between an Internet user and a web server stored in a file on the user's hard disk. So they can be used to monitor Internet activities of the user.

The previous privacy legislation required websites to give users information on how they could remove or opt-out of cookies, which was commonly placed in privacy policies that went mostly unread. With the EU Cookie Directive the user of a site will now be required to opt-in when using a website containing cookies. So the website has to block cookies, until visitors have given their informed consent to their use.

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 authorised personnel for legally authorised purposes,"
- "protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,"
- "ensure the implementation of a security policy with respect to the processing of personal data"

2.1.4 Electronic Signatures

In this context, it is worth to mention the Directive 1999/93/EC on the Community Framework for Electronic Signatures, because the concept of privacy is strictly coupled with an 'identifiable person', and this directive makes the electronic signature, when implemented in compliance with the directive, a recognised tool for the legal identification of a person.

This Directive establishes the legal framework at European level for electronic signatures and certification services. The aim is to make electronic signatures easier to use and help them become legally recognised within the Member States.

The Directive defines two new ideas: the advanced electronic signature and the qualified certificate. The main provision of the Directive states that an advanced electronic signature based on a qualified certificate satisfies the same legal requirements as a handwritten signature. It is also admissible as evidence in legal proceedings. Furthermore, this Directive lays down the criteria that form the basis for legal recognition of electronic signatures by focusing on certification services, namely:

- common obligations for certification service providers;
- common rules on liability to help build confidence among users;
- and cooperative mechanisms to facilitate trans-border recognition of signatures and certificates with third countries.

2.2 National Legal Framework for Privacy Protection

The paragraphs below explain how each of the countries involved into the pilot execution implement, through laws and regulations, the EU Directives described above.

2.2.1 Turkey

The ‘e-Transformation’ 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). Moreover, Electronic Signature is granted legal recognition with the Turkish Law No 5070 in 2004. The access to the electronic services are supposed to be provided by the state through the Turkish Law on Free Access to the Services (Law No: 5369, Official Gazette No: 25856).

As the electronic communication becomes widespread, so does the offences, crimes and cyber-attacks, hackings etc…Consequently a legislation was enacted in 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 Right to Access Information that was published in Official Gazette in 2003 (Law No: 4982). However the privacy issues and commercially classified information is protected by a few 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). The acts and actions against the mentioned laws and regulations require legislative actions that are

codified in Turkish Penal Code (Law No: 5237, Official Gazette No: 25611) and Turkish Law on Civil Servants (No:657 ,Official Gazette No:12056).

The area in and around military zones and high security areas are regulated by Turkish Law no 2565 (Official Gazette No: 17552, Dated 1981).

2.2.2 Serbia

Protection of personal data is guaranteed by the Constitution of the Republic of Serbia. Law on Personal Data Protection (Official gazette of the RS 97/08, 104/09, 68/12) is highly harmonized with the EU legislature.

The Law clearly defines the cases when processing of personal data is not allowed, as reported below:

Inadmissibility of Processing

> ***Article 8***
>
> *Processing shall not be allowed:*
>
> *1) If a natural person did not give his/her consent to processing, i.e. if processing is carried out without legal authority;*
>
> *2) If processing is done for purposes other than those specified, regardless whether it is based on a person's consent or on statutory powers for data processing without consent;*
>
> *3) If the purpose of processing is vaguely defined, modified, inadmissible or already achieved;*
>
> *4) If the data subject is identified or identifiable even after the purpose of such processing is achieved;*
>
> *5) If the processing method is inadmissible;*
>
> *6) If the processed data is unnecessary or unsuitable for the purpose of processing;*
>
> *7) If the number or type of data processed is disproportionate taking into account the purpose of processing;*
>
> *8) If the data are inaccurate and incomplete, i.e. if they are not based on a credible source or are outdated."*

However, the Law recognizes personal data that are excluded from the scope of the Law:

> ***Article 5***
>
> *Save where a person's contrary interests manifestly prevail, certain provisions of this Law pertaining to processing requirements and to the rights and responsibilities in connection with processing shall not apply to the processing of:*

1) Data available to everyone and published in mass media or publications or accessible in archives, museums and other similar organizations;

2) Data processed for family purposes and other personal purposes which are unavailable to third parties;

3) Data on members of political parties, associations, trade unions and other forms of alliances processed by such organizations, provided that the member concerned has given his/her consent in writing to waive the application of certain provisions of this Law to his/her personal data for a specified period of time, which however cannot exceed the term of his/her office;

4) Data published on oneself by a person capable of taking care of his/her interests."

There are, however, cases when consent of the persons is not required:

Processing without Consent

Article 12

Processing without consent shall be allowed in the following cases:

1) To achieve or protect vital interests of the data subject or a third party, in particular their life, health and physical integrity;

2) For the purpose of discharging duties laid down by a law, an enactment adopted pursuant to a law or a contract concluded between the person concerned and the controller, as well as for the purpose of contract preparation;

3) In other cases envisaged by this Law or another regulation adopted pursuant to this Law, for the purpose of achieving a prevailing justifiable interest of the person concerned, the controller or a user.

Processing by Public Authorities

Article 13

Public authorities shall process data without the consent of the person concerned if such processing is necessary for them to perform duties within their spheres of competence as defined by a law or another regulation with a view to achieving the interests of national or public safety, national defence, crime prevention, detection, investigation and prosecution, economic or financial interests of the state, protection of health and ethical norms, protection of rights and freedoms and other public interests, while processing in all other cases shall require the consent in writing from the person concerned.

Other laws related to the same subject, which it is worth to mention are:

- the Data Secrecy Law ("OG RS" 104/09)
- Law on Electronic Signature ("OG RS" 135/2004)
- Law on the Organization and Competences of Government Authorities for High-Technology Crime Control ("OG RS" 61/05)

- the Criminal Law ("OG RS" 85/05, 88/05, 107/05, 72/09, 111/09).

2.2.3 Greece

The protection of privacy is achieved through the protection of personal data. The Greek Law 2472/1997 on the "Protection of the individual against processing of personal data" has adopted the definition of personal data set by the Directive 95/46/EC. The keynote principles provided by the above-mentioned Law can also be applied in the personal data processing in electronic communications, on condition that they are appropriately modified.

However, the protection of personal data and privacy in the telecommunications' sector, including electronic communications services in public communications networks, is further specified by the Greek Law 3471/2006. This Law constitutes the implementation of the Directive 2002/58/EC, which refers to the processing of personal data and the protection of privacy in electronic communication.

The Law 2472/1997 dictates that the personal data of electronic communications' users or subscribers (Arkouli, 2011):

- Should be collected fairly and lawfully.
- Should be accurate, true, and –where necessary– kept up to date (principle of accuracy).
- Should be collected for specified, explicit and legitimate purposes and should not be further processed in a way incompatible with those purposes (principle of scope).
- Should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, according to the "principle of necessity". The "principle of necessity" of personal data processing occurs also in the Law 3471/2006 in a harsher phrasing. Under this principle, personal data processing should be restricted to the extent that is absolutely necessary for the sort and the purpose of the processing. Moreover, the providers of publicly available electronic communications services must take the appropriate technical measures and must design and select the appropriate information systems in order to process the absolutely necessary personal data.

Additional general principles of personal data protection were also incorporated in the more recent Greek Law 3979/2011 entitled "On e-Government and other issues", which regulates the use of information and communication technology by the public organizations and institutions for their transaction within the public sector and between the public sector and the private one. The basic general principles of the Law 3979/2011 (articles 7 and 8) are the following:

1. The organizations of the public sector offering e-Government services should respect the right of the protection of personal data and privacy of individuals.

2. The effects of information systems and e-Government services to the privacy and to personal data protection should be evaluated during the design, the formulation and the procurement of such systems of services.

3. The design, formulation and procurement of information systems and e-Government services should take into consideration the right of personal data protection and the necessity to configure these systems and services in a manner that ensures the processing of the minimum personal data.

4. In the cases defined by this Law, in which the individual's consent is required for the processing of personal data, this consent can also be declared through the use of information and communication technology. The public organization should safely preserve the declaration of consent in a way that it is always accessible. The declaration of consent can be withdrawn any time, but without any retroactive result.

5. The further use of personal data, for statistical purposes or for the amelioration of the services offered, is allowed provided that this data is rendered anonymous.

2.2.4 Italy

In Italy, the ordinary legislation on privacy is contained in Legislative Decree 30 June 2003, 196: Code concerning the protection of personal data, commonly known as "Unique Act on Privacy."

Legislative Decree 196/2003 repeals the previous law 675/96, which had been introduced, in May 1997, to meet the Schengen Agreement. On the directive enforcement oversees the Guarantor for the Protection of Personal Data, an administrative authority established since L. 675/1996, then confirmed by the Act of 2003.

The various tasks of the Guarantor (art. 154 Leg. 196/2003) include those of:

- check that the personal data treatments are undertaken in accordance with the law
- receive and investigate complaints and reports submitted by interested, and express opinions in the cases reported
- prohibit illegal or improper treatments and possibly dispose the block
- promote the signing of codes of ethics and good conduct of certain sectors
- report to the Government and Parliament the opportunity to issue new regulatory measures demanded by the sector
- treat the public understanding of the regulations governing the processing of personal data and its aims and measures in the field of data security
- report the facts configurable as offenses prosecutable 'ex officio'
- keeping the register of processing of personal data
- prepare an annual report on its activities for submission to the Government and Parliament

- be consulted by the Government or Ministers when they draw up rules that affect the subject

The Art.1 of the Decree pertains to the rights of personality, stating that "Everyone has the right to protect personal data concerning him."

Art 3 defines the 'principle of necessity of data processing' and refers to information systems and computer programs, which have to be configured in order to reduce as much as possible the use of personal data and identification data, so as to exclude the treatment when the purpose in each case can be achieved by using anonymous data or mechanisms that allow identification of the individual only in case of necessity.

The purpose of the law is to avoid that the data are processed without the consent of the person entitled, so as not causing injury. In the articles from 8 to 10, for this purpose, are defined the rights of individuals, the collection process and data requirements, the obligations of who collects, holds and processes personal data, liability and penalties for damage.

The Legislative Decree no. 69/2012 amends Legislative Decree 196/2003 and includes the implementation of the European Cookie Directive. Beyond this, it specifies the issue of 'expression of consent', declaring that personal data treatment is permitted if "the contractor or user concerned has given his or her consent" (Article 122). The Decree specifies also "in order to express the consent, specific configurations of computer programs or devices that are easy and clearly usable for the contractor or the user may be used"

The Digital Administration Code (Italian Legislative Decree 7 March 2005, n. 82), treats the data privacy issues in relation to the electronic transactions involved into the e-Government flows. In particular Art. 29, 'Privacy of data transmitted electronically', says: "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".

2.2.5 Croatia

Protection of personal data is guaranteed by the Constitution (Article 37 of the Constitution of the Republic of Croatia). In 2003, Croatia adopted the Act on Personal Data Protection (the "Act"), which it subsequently amended in 2006, 2008 and 2011. The Act on personal data protection has been passed on the basis of the constitutional provision on the right to personal data protection (Official Gazette N° 103/03, 118/06, 41/08). The Act on personal data protection as a basic law in the field of personal data protection in the Republic of Croatia has also been harmonised in all relevant provisions with the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. For example, international data

transfers outside of Croatia are only allowed when an adequate level of protection of personal data is ensured. Additionally, the Act requires data controllers to maintain records of their processing activities, which must be submitted to the Personal Data Protection Agency for compilation in a Central Register. This generally corresponds to the notification obligation under the Data Protection Directive. For certain specified violations, the Act establishes fines in the amount of HRK 20,000 to 40,000 (approximately €2,700 to €5,400).

In addition, Croatia has enacted several specific laws regulating the personal data protection domain:

- the Electronic Communications Act implements the e-Privacy Directive 2002/58/EC, as amended by Directive 2009/136/EC
- Regulation on the manner of keeping the records of personal data filing systems and the pertinent records form (Official Gazette N° 105/04) and
- Regulation on the Procedure for Storage and Special Measures Relating to the Technical Protection of Special Categories of Personal Data (Official Gazette N° 139/04), which sets forth detailed information security measures.
- Electronic Signature Act (NN 10/02, 80/08); Ordinances of the Ministry of Economy, Labour and Entrepreneurship - based on Directive 1999/93/EC.

The Croatian Personal Data Protection Agency monitors compliance with the Act on Personal Data Protection.

3 Privacy Protection in e-Government Services

Beyond the legal framework, it is interesting to consider all the guidelines, directives and procedures established within Public Administration for the implementation of the legislation related to privacy and data protection and its application to e-Government services.

This chapter aims to offer a panorama of the practices adopted at European level, through the description of the approach, in terms of procedures or technical solutions (protocols, data management) followed in each of the pilot countries and applied by the involved local authorities for the e- Government solutions to ensure privacy and data-protection.

The chapter also includes an analysis on the impacts of the cloud on the privacy issue, and, finally, provides an overview of the guidelines that apply in each of the pilot countries towards the adoption of cloud solution for e-Government services.

3.1 Best Practices for the Management of Sensitive Information

3.1.1 Turkey

There is not a specific regulation in place for the protection of personal data in Turkey that translates the law into procedural and technical practices; each local authority, therefore, applies its own management system. In this regard, Ministry of Environment and Urbanization and therefore NCEDTR apply an in house system and keep the sensitive information within their intranet.

They also follow the 27001 data security standards and use authentication, validation and password encoding for the safety. In addition to that, logging and firewalls are commonly used.

Furthermore, the department of population and citizenship affairs department, established within the Ministry of Internal Affairs, developed the portal for the National ID numbers, which provides the best security standards for the protection of personal data.

If any of the government agencies or local authorities would like to use the web-services from this application needs to meet the below requirements:

- XML Web Service calling (SOAP 1.2)
- WS-Security 1.1, WS-Trust 1.3 and WS-SecurityPolicy 1.2 for web service security
- Newly developed version of the portal uses the Single Sign On – SSO method for the authentication .Web service user needs to use (Security Token Service – STS)
- STS, WS-Security - UsernameToken security systems applies and, at transport level, SSL (secure sockets layer) is in use.

IP Limitation is another common method for the security.

3.1.2 Serbia

Practice adopted by the Municipality of Indjija in order to manage sensitive information is to store the information on the internal servers. No information is being published; they are only used by internal applications via intranet structure. The only people who have access to it are the authorized public servants.

Some of the data is available to the people to whom it applies, and this is done through username/password interface on the Municipality's website.

Examples of best practices of e-Government in Europe were part of the study of the Estonian e-Governance Academy from Tallinn about the e-Government activities in 2007, one of which was the Municipality of Indjija.

All sensitive data used in the work of public authority through software developed by the Municipal Agency for IT, GIS and Communication are available in an intranet structure, therefore the only access enabled is for the servants who are authorized to work with the data. All web-based applications are hosted on the municipality's servers and no providers' services are being used, so intranet protection is at the level of username and password. This is due to the fact that the Agency's central firewall regulates input/output traffic, so it is not possible to gain unauthorized access from the outside.

The only interface that enables outside users to access personal data is the web site where the users, knowing their parameters can access some of their personal data. For this purpose the HTTP protocol is being used, through which the encryption of the traffic in the open client-server session is being done.

The Agency has also developed a software solution for authentication through smart cards and certificates issued by the official certification authority.

3.1.3 Greece

The Region of Crete, being a Greek self-administration organization (NUTS Level II), currently uses a series of e-Government services created and provided by the competent Ministries of the Greek Government. Two of the most widely used e-Government services are:

- "CL@RITY", which constitutes a major transparency initiative and innovation of the Ministry of the Interior, Decentralization and e-Government of Greece. In fact, since October 2010, the decisions of the public entities cannot be implemented if they are not uploaded on the "Clarity" websites, with the exception of decisions that contain sensitive personal data and/or information on national security. The term "sensitive personal data" is defined in the Greek Law 2742/1997 on the protection of personal data as "the data concerning the racial or national origin, the political convictions, the religious or philosophical beliefs, the participation in union organizations and corporations, the health, the social welfare and the sexual

life as well as the data related with criminal prosecutions or condemnations" (article 2). This type of sensitive personal data is irrelevant to issues which concern environmental permitting processes and environmental terms of projects and activities.

- The "geodata.gov.gr – Public data, open data" service, which constitutes the first attempt for free disposal of the geospatial data which is available to the public administration to all citizens of Greece. This service was developed by the Institute of Information Systems.

According to the terms of use and the data protection policy of the above described e-Government services, their owners / managers (i.e. the Ministry of the Interior, Decentralization and e-Government and the Institute of Information Systems respectively):

- Can collect "personal data" solely of the users of visitors of the website. The term "personal data" is defined here as "the set of data which can be used only for the identification of the users and visitors of the website, or for the contact with them". The user or visitor of each website unconditionally consents to provide the above personal information to the respective website, where required or requested and the owner / manager of the website can use this data for informational purposes or for e-mailing the subscribed user or visitor, unless he / she would not like that.
- Do not sell personal data of third parties or of the users and visitors of the websites. Neither do they transfer or publish personal data, unless there are different provisions by the rule of law, or unless it is necessary for the effective function of the website.
- May elaborate part of or all the data provided by the users and visitors for statistical purposes and in order to improve the services and information provided through the websites.

Additionally, the Region of Crete has created the website crete.gov.gr, which offers various information and services to the public, on the terms and conditions of the Greek legislation concerning the protection of privacy and personal data. Each visitor or user who would like to use any of the services provided by the website should create his / her own username and a password and is obliged to provide true, accurate, valid and complete information and keep it up to date, so that it remains true, accurate, valid and complete.

3.1.4 Italy

The best practices that apply in Italy for the protection of privacy of citizens in the e-Government system are those defined by the Guarantor for the Protection of Personal Data in the Resolution of 25/01/2012. Within this resolution, the Guarantor has established, for all the public web sites, a set of practical rules to prevent the risks

associated with improper disclosure of personal information of the users involved and to encourage greater awareness on the part of the users themselves. The e-Government services adopt the same set of rules.

e-Government services that require registration data (name , email address , date of birth, etc.) to citizens, have to comply with the obligation to inform interested people about the purposes of collecting data and storage times, specifying which data are optional, and if the input data can also be viewed by non- registered or via search engines (e.g. Google or Yahoo). Rights concerning the cancellation or correction of entries must also be safeguarded. The user must explicitly confirm that this information has been read and understood.

All the public web-sites (i.e. also those who do not require the recording of the user) must include a special "warning" that draws attention to the risks that can occur by entering sensitive data both at the time of registration and in the later stages. Just to ensure the confidentiality of the people, it is allowed to use a nickname (instead of its name) and the e-mail address will not automatically be posted on the site along with user comments. It will also be advised not to enter data, photos or video that make it easier to identify (e.g. references to e-mail boxes, places, people, circumstances that allow even indirectly traced back to its identity), and this also applies for other people who might be united to the author of the post.

The data requested and then collected by the site operator must be protected by appropriate security measures to minimize the risk of loss, even accidental, unauthorized access, treatment not allowed . These data should not be disclosed to third parties.

3.1.5 Croatia

The current practice does not include harvesting, analysis or publication via Internet of any sensitive information. Only the information that is classified as public is being published. Sensitive information is submitted on the requested location in hardcopy and is being registered and controlled by appropriate administrative procedures.

The technical solutions defined in legislation that is currently being implemented by the e-Croatia office include the following:

- National electronic identity management infrastructure with central gateway for authorisation and authentication for users of on-line services
- Criptologic protection
- Electronic signatures
- National ID on a smart card

It is mandatory that all measures, procedures and staff authorised for system safety, storage and protection need to be in line with the respective international recommendations (ISO17799).

3.2 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. Data protection and identity management, therefore, become increasingly important to assure continued trust in these services and the uptake of them.

Governance models and processes need to take into account the specific issues arising from the inherently global nature of the Cloud.

Although the European Digital Agenda promotes the development of an EU-wide strategy on cloud computing, the current legislation, both at European and at local level, does not explicitly 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 the uncertainty in the design of the Cloud e-Government solutions. The requirements to take into consideration while designing an e-Government service on the cloud, and, in the same way, when the subject is the privacy protection, consequently, are those related to the management of data. Data is subject to specific legislative requirements that may depend on the location where they are hosted, as well as for what purposes they are processed. In the Cloud case, therefore, there is a lack of clarity on the applicable law, because the data subject, the data, the controller, the processor and the processing may be located in different countries.

Different countries have different laws regarding which kind of data may be hosted, where and how it is to be protected and may be accessed or made public. Within the Cloud, data may be hosted anywhere within the distributed infrastructure, i.e. potentially anywhere in the world.

Privacy protection is one of the main concerns to take into account in the design of e-Government services to be deployed on the Cloud, as trust in Cloud computing is a key prerequisite.

Among the barriers for the adoption of the 'e-Government 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 when different rules (e.g. regarding data location) have to be obeyed, is one of the most outstanding from the service provider point of view.

That is why, the recommendation drafted by the industry workgroup to the European Commission on the orientation of a Cloud computing strategy for Europe (see [7]) 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.'

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

1) *The EC should ensure that 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.*

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.*

Definitely, as it's not possible to wait that the EC takes the required legislative action to start the implementation of the eEnviPer system, the impact of the cloud computing environment on the data protection issues has to be minimized, applying, if necessary, restrictive policies.

The eEnviPer system 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, as minimum requirement, establish the fact, in particular, 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 might not communicate the data to third parties, even for preservation purposes.
- 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 organisation and data processing arrangements (and those of its subcontractors, if any) are compliant with the applicable national and international legal requirements and standards.

Furthermore, 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 eEnviPer service entirely within each single country in which it is delivered, and to ensure that the data does not go beyond the boundaries of that country. The location of data storage/processing, in fact, affects directly both on the applicable law – in case of disputes between client and provider – and on the national rules applying to data processing, storage, and security. It is clear that acting in strict compliance with this requirement can be a limitation for the service, as most of the cloud providers do not have a hosting centre in each European country, as this would not be a cost-effective choice.

Privacy laws, however, only allow "exporting" data from the EU under specific circumstances and if adequate protection measures are in place for data subjects by comparison to the protection afforded under EU legislation. Thus, a cloud-based service might entail unforeseen additional costs resulting from the client's limited control over his data, or else – which is more likely – because of national and international litigation.

With respect to the geographic location of data, therefore, a good compromise, for an eEnviPer service activated in one of the EU states, would be setting, as a minimum requirement, the obligation to store the data of the service within the EU borders, and provide guarantee that they will not be transferred outside.

The table below illustrates the attitude of public authorities towards e-Government cloud-based solutions, and the related potential privacy issues, in the pilot countries.

Table 1: Attitude towards cloud-based e-Government solutions in the pilot countries

Pilot Country	Comment
Turkey	Public Authorities signs a protocol (agreement) in order to join the e-Government gate portal and determines the rules according to the protocol. There is not any specific regulation or method for cloud-based solutions. However, same security standards, which the Ministry of Interior applies, are required. IP limitation and site-to-site VPN connection are also used by the public authorities.
Serbia	Several laws and strategic documents cover the area of privacy protection, but not many strictly addressing the cloud-based solutions. "Information Society Development Strategy in the Republic of Serbia until year 2020" (51/2010) states in the chapter "eCommerce" that new

Pilot Country	Comment
	technological trends should be taken into consideration, and that "special attention should be given to the development of the cloud computing". The same document addresses several other aspects related to e-Government and protection of privacy, and calls to several relevant laws. In a chapter concerning e-Government, it states that by the year 2020, citizens will be able to make all contacts with public authorities, that by nature require physical presence, by electronic means. The same chapter considers the usage of qualified electronic certificates as the main mean of identification, as it is regulated by the Law on Electronic Signature (Official Gazette of the RS 135/2004), as Electronic signature secures appropriate functions, such as authenticity, integrity and legality, in accordance with the legislation. In relation to this, the chapter states the significance of interoperability of e-signature and e-identity with other countries, especially EU member states. It also states that development of e-Government is pointed to, among other goals, protection of privacy and security. The chapter concerning the information safety states that the goals of the development of the information safety are, among others, protection of data and efficient mechanisms of protection of rights in processes of e-business and electronic data exchange.
Greece	The rules for privacy protection and processing of personal data were clearly set by the Law in 1997. These rules have been since then generally applied to all fields and sectors and later, in 2006, were also adopted by and partly modified for the needs of the privacy protection in the field of electronic communication. The Law that integrated the general principles of the protection of personal data in the field of e-Government was published in 2011 (Law 3979/2011). However, the Law 3979/2011 refers to e-Government in general, with no strict reference to privacy protection or other rules, which should be applied in the case of cloud-based solutions. The design and development of the e-Government legislation frame and implementation is the main mission of the Ministry of Administrative Reform and e-Government. The Ministry has thus created the "road map" of the e-Government implementation, which is considered as the only way to spot the amendments, specifications or completions of the Law 3979/2011. This "road map" includes, among other plans and targets, the creation of a national login service and the plan to provide the staff of the public organizations with e-signatures.

Pilot Country	Comment
	Therefore, until any amendment of the Law 3979/2011 or the publication of any new Law or strategic document, which will refer strictly to the processing, and protection of privacy in cloud-based solutions, the currently valid general privacy protection rules should self-evidently be applied.
Italy	In Italy, the Guarantor for the Protection of Personal Data produced some documents about the matter. Among the others it is worth to mention "Cloud Computing - Protect your Data Without Falling from a Cloud", which includes specific examples and a Decalogue with practical tips and suggestions for further analysis. Businesses and public bodies can rely on this tool to start probing into the potential risks of cloud computing and decide what data should be moved to the cloud for what purposes. The tips of the Decalogue are reported hereinafter: 1. check how reliable your provider is 2. prefer services with enhanced data portability (i.e. rely on open formats and standards to facilitate migration between cloud systems managed by different providers) 3. make sure data is available whenever necessary 4. select which data should be moved to the cloud 5. never lose sight of your data 6. know the physical location of your data 7. be alert to your terms of service 8. check for how long and in what manner data is retained 9. demand adequate security measures 10. train staff appropriately
Croatia	There are no legal or technical practices in place specific for regulating privacy in e-Government cloud-based solutions. Therefore, the already mentioned laws (see 2.2.5) that regulate privacy and privacy preservation apply. These laws (like the Directive) does not define the technological level, they are technology neutral In addition, a number of capacity building EU funded projects were undertaken to raise awareness about the benefits of e-services (for example the "E-business competitiveness improvement programme" focused on developing a better understanding in SMEs of the importance and applicability of e-business tools as a means to achieving competitiveness with privacy issues being addresses through workshops and training materials developed).

4 Privacy Protection Issues in the eEnviPer Data Flows

The present section aims to identify the potential data protection issues identified in the data flows involved in the use cases designed for the eEnviPer system. The information collected here, therefore, had the purpose to take into consideration for the design of the technological solution and the user's functionalities.

With this objective, the partners responsible for the definitions of the workflows have been asked to identify, for each step, the nature of data involved and the actors between which data are exchanged.

The data involved in the electronic permitting procedure have been identified and classified according to the privacy level as follows:

- Personally Identifiable (PI) / Non-Personally Identifiable (NPI)
- Sensitive (S) / Non-Sensitive (NS) / Highly-Sensitive (HS)

In addition, the data flows through which these data are exchanged are classified into the following categories:

A) moving intra-departmentally or intra-personally within the single organisation responsible for the permit release

B) moving between different organisations responsible for the permit release

C) moving from the organization to third parties

D) received by the organisation from third parties

E) moving across state / national boundaries

Once identified data and exchange flows, the potential privacy issues have been detected by matching the operational activity connected with the use cases with the privacy checklist reported in [A].

In accordance to this approach, the paragraphs below identify and classify, for each of the pilot countries, the data treated by the eEnviPer system, and indicates the potential privacy issues either in the use cases of the workflows designed, or in the pilot execution or project exploitation phases.

4.1.1 Turkey

Data handled by the system and information flows related

Information type	**Category (PI,NPI /S, NS,HS)***	**Data Flow Category Mapping**
Applicant Name, Business Address, Communication Information,	PI/S	From Firm/Engineer/Owner to the Province Department (D)
Environmental Firms/Engineers Name/Company Name	PI/S	From Firm/Engineer/Owner to the Province Department (D)
Firm/Engineer's Address/Tel/Fax/e-mail	PI/S	From Firm/Engineer/Owner to the Province Department (D)
Project Location/Address/Coverage Area	NPI/HS	From Firm/Engineer/Owner to the Province Department (D)
Project Size/Capacity/Investment Amount/Classification	NPI/HS	From Firm/Engineer/Owner to the Province Department (D)
Application File Submission Date	NPI/HS	From Province Department to Ministry as part of Reporting Requirements (B)
Applicants File Check Results, Missing Documentations, Types of Missing Documents	NPI/HS	From Province Department to the Environmental Firm/Engineer (D)
Number of Submittals and Transmittals for Application File Completion/Correction and the Transmission Dates of Submittals and Transmittals	NPI/HS	From Province Dept. to the Environmental Firm/Engineer and vice versa (C, D)
Submitting Revised Application File with more detailed documentation.	NPI/HS	From Agent/Owner to the Province (D)
Provincial Decisions/Dates	NPI/HS	From Province to the Agent (C)
Provincial Department Staff File and Field Checks/ Check Dates/Department Evaluation/Letters to the Firm/Engineer for Penalties (if any)/Completion Notice	NPI/HS	From Province to the Firm/Engineer/Owner (C)
If during the field check any unpermitted/unlicensed activity is found, the provincial department issues fines/penalties of certain amount listed in legislation	NPI/HS	From Province to the Firm/Engineer/Owner (C)
After the evaluation/check and confirmations done; ' EIA not required' status is granted to the application, and the a form is issued to the applicant/The date of Issue	NPI/HS	From Province to the Firm/Engineer/Owner (C)

Use cases vs Privacy Issues

Use case that can trigger the issue	**Transaction, stakeholders involved, data/information exchange**	**Privacy issue that can arise**	**National and/or EU legislation addressing/regulating the issue (if exists)**
All	Data Sharing with the relevant authorities and other administrative units	Leak of Personal./Classified Info	Decree on Protection of Commercial Secrets and Access Rules to the Commercial Information No:2010/3 Turkish Law No:2565 – Military Zones and Highly Security Areas 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
11.001	Administrative Evaluation Procedures	Biases of the Provincial Staff that leads economical loss of the investor	Turkish Law on Environment o:2872/1983 Regulation on Environmental Impact Assessment/2008 Turkish Law on Civil Servants No:657
11.001	Province asks for the completion of the application file from the agent/owner	Submittals/Transmittals /Letters are bypassed and the traceability is lost	Turkish Law on Civil Servants No:657
All	EIA Study is Submitted by the Licensed Environmental Consulting Firms or	Application File Contains Forged Documents/ The documents fabricated	Article 204,205,206 and 207 of the Turkish Penal Code No: 5237/2004

Use case that can trigger the issue	**Transaction, stakeholders involved, data/information exchange**	**Privacy issue that can arise**	**National and/or EU legislation addressing/regulating the issue (if exists)**
	Engineers on behalf of the Applicant The province requests missing documents/corrections from the applicant	by the Environmental Firms/Engineer.	
12.001	The Provincial Department Staff reviews the application letter and decides on the Requirement of EIA	The provincial department staff takes a wrong decision due to misinformation, or lack of competent officers for satisfying checking standards	
All	Electronic Data Usage (Uploading, exchanging documents, GIS data etc.)	Viruses can infect to system, damage data and circumvent data security	Turkish Law No 5809 – Law on Electronic Communication Turkish Law No: 5651 – Regulating the internet transmission issues and combating the crimes which are conducted by internet transmission
	Publishing GIS Data of the Location of Interest	Confidential Information, Classified Information of Highly Sensitive Military Zones	Turkish Law No:2565 – Military Zones and Highly Security Areas
16.001	Submitting the Bank Receipt to the Commission with a letter	The bank receipt could be forged	Article 204,205 of Turkish Criminal Law No:5237 : Forgery

4.1.2 Serbia

Data handled by the system and information flows related

Information type	**Category** **(PI,NPI /S, NS,HS)***	**Data Flow** **Category Mapping**
Name and address of the investor (company) and name of the authorized person (director/manager)	PI, NS	A, C
Title of the project and short technical description	NPI, NS	A, C
Cadastral parcel(s) ID and Cadastral Municipality name	NPI, NS	A, C
EIA study (technical and legal information)	NPI, NS	A, C
Name of the consultant (expert) who is the author of the EIA study on behalf of investor	PI, NS	A, C
ID number of case/decision	NPI, NS	A, C
Decisions of the Authority	NPI, NS	A, C
Complaints of the investor	PI, NS	A, D
Request for additional data by the Authority	PI, NS	A, C
Internal reports and opinions of the Authority	NPI, NS	A
Complaints of citizens	PI, NS	A, C, D

Use cases vs Privacy Issues

Use case that can trigger the issue	**Transaction, stakeholders involved, data/information exchange**	**Privacy issue that can arise**	**National and/or EU legislation addressing/regulating the issue (if exists)**
Use case 9, Influence of the public	A citizen leaves a comment or a complaint on a EIA application.	Employee who is authorized to approach the system misuse personal data of the user (email address, name,…)	Law on personal data protection (Official gazette of the RS 97/08, 104/09, 68/12)
Any use case	Any transaction	The cookies stored in a user's browser can allow tracking of the users activity on Internet	Directive 2009/136 There is no national legislation addressing this issue.

4.1.3 Greece

Data handled by the system and information flows related

Information type	**Category** **(PI,NPI /S, NS,HS)**	**Data Flow** **Category Mapping**
Type of the activity-project	***NPI, NS***	D, B, A, C
Classification and extent (size) of the activity-project	***NPI, NS***	D, B, A, C
Information about legal entity/person (owner, administrator)	***PI, NS***	D, B, A, C
Information about Studier, EIS manager	***PI, NS***	D, B, A, C
Environmental Impact Study (as a whole)	***NPI, NS, but:*** i) Intellectual property restrictions should be taken into account. ii) In case that data or information necessary for the EIS or the Environmental Report, fall into restrictions of commercial confidentiality or protection of inventions and industrial design, the Expert who carried out the EIS has to site them, so that they are not published in any way during environmental permitting and approval.	D, B, A, C
Spatial data of the activity-project	***NPI, NS***	D, B, A, C
Drawings and maps of the installation field and the broader region	***NPI, NS, but:*** i) Intellectual property restrictions should be taken into account. ii) In case that data or information depicted on the drawings or maps, fall into restrictions of commercial confidentiality or protection of inventions and industrial design, the Expert who carried out the EIS has to site them, so that they are not published in any way during environmental permitting and approval.	D, B, A, C
Information about the technical background of the activity or project	***NPI, NS, but:*** In case that data on the technical background fall into restrictions of commercial confidentiality or protection of inventions and industrial design, the Expert who carried out the EIS has to site them, so that they are not published in any way during environmental permitting and approval.	D, B, A, C
Photographs of the project's location site	***NPI, NS, but:*** In case that subject of photographs falls into restrictions of commercial confidentiality or protection of inventions and industrial design, the Expert who carried out the EIS has to site them, so that they are not published in any way during	D, B, A, C

Information type	**Category (PI,NPI /S, NS,HS)**	**Data Flow Category Mapping**
	environmental permitting and approval.	
Opinions on the EIS expressed by public authorities	***NPI, NS***	B, C
Opinions on the EIS expressed by the public (citizens, NGOs, other stakeholders)	***PI, NS***	D

Use cases vs Privacy Issues

Use case that can trigger the issue	**Transaction, stakeholders involved, data/information exchange**	**Privacy issue that can arise**	**National and/or EU legislation addressing/regulating the issue, if exists**
Public consultation 3K001	**Publicizing Environmental Impact Studies, information and data on projects and activities, so that the citizens, Non-Governmental Organizations and other stakeholders have access and may express their opinion**	Protection of personal data, of copyrights and intellectual property and the access to environmental information Providing information on the project (type, raw materials, industrial design, production line etc.). In case that data or information necessary for the EIS or the Environmental Report, fall into restrictions of copyrights or protection of inventions and industrial design, the Expert has to site them, so that they are not published during environmental permitting and approval.	a) Greek Law 2472/1997 & 3471/2006 for the protection of personal data b) Greek Law 2121/1993 concerning the copyrights c) Common Ministerial Decision 77921/1440/1995 concerning the access to environmental information.
All	**Free disposal of spatial data (geodata) of the Public Administration to all citizens of Greece**	There should be open access to all the spatial data provided by our system.	Greek Law 3882/2010 and EU Directive 2007/2/EU (INSPIRE Directive)
2ΣΑ03α 2ΣΑ03β 2ΣΑ03γ	**Self-imposed search of documents be the public authorities, use of information of the public sector**	Use of permitting process documents in the possession of the public sector. Occasionally some types of documents might be needed during environmental permitting process and environmental control, which fall into the categories of documents to be asked for automatically by the public authorities from the competent authorities, without	Greek Law 3448/2006

Use case that can trigger the issue	**Transaction, stakeholders involved, data/information exchange**	**Privacy issue that can arise**	**National and/or EU legislation addressing/regulating the issue, if exists**
		any citizen's intervention	
Public consultation	**Public debate** Publicizing the EIS, so that the citizens, Non-Governmental Organizations and other stakeholders may express their opinion Publicizing the data and information provided by the owner of the project or activity	Access of the public to project's data, alternative solutions and environmental impact of the project Informing the public that they may have access to the EIS, so that they express their opinion The competent environmental Authority sends information and data to the Committee of the Region, so that they publicize it and inform the public, but the conduct of public debate procedure is not mandatory	a) Greek Law 2472/1997 & 3471/2006 for the protection of personal data b) Greek Law 2121/1993 concerning the copyrights c) Greek Law 1733/1987 concerning the protection of inventions and industrial design. d) Common Ministerial Decision 77921/1440/1995 concerning the access to environmental information.
Publication of the Environmental Permission	**The competent Environmental Authority issues the Environmental Approval or renewal or amendment decision**	There should be open access to the outcome of the Environmental Permitting Process, renewal or amendment of the Decision of the Environmental Approval: publication on the CL@RITY website.	a) Common Ministerial Decision No. 77921/1440/1995 on the free access of the pubic to Authorities concerning environmental information b) Greek Law 3861/2010 for administrative decisions' publication on the CL@RITY website.
Correspondence between Authorities (including the Legal Authority 1A012 1A032 1A050	**i) Request to express opinion on the EIS** **ii) Opinion expressed** **iii) Evaluation of the opinion by the Environmental Authority** **iv) Consideration of the opinions expressed in issuing the Environmental**	1. When necessary, the Environmental Authority has the right to ask other competent Authorities to express their opinion on the EIS. 2. When requesting other competent Authorities' opinion, the Environmental Authority should provide them with all necessary information and data for their objective and unbiased	a) Greek Law 4014/2011 b) Greek Law 2690/1999 c) Greek Law 3242/2004 d) Greek Law 2472/1997 & 3471/2006 for the protection of personal

Use case that can trigger the issue	Transaction, stakeholders involved, data/information exchange	Privacy issue that can arise	National and/or EU legislation addressing/regulating the issue, if exists
	Approval	opinion. 3. All Authorities involved should take into account protection of personal data, restrictions of copyrights and (if necessary) protection of inventions and industrial design.	data e) Greek Law 2121/1993 concerning the copyrights f) Greek Law 1733/1987 concerning the protection of inventions and industrial design.
1A011	**Correspondence with the owner of the project of activity (e.g. to ask for additional data and information)**	The environmental permitting process cannot be integrated, unless all necessary data and information is provided by the owner of the project or activity.	Greek Law 4014/2011 Greek Law 2690/1999 Greek Law 3242/2004

Potential Privacy Issues in the Pilot Execution & Post Exploitation Scenario

Privacy issue and the action that can trigger the issue	National and/or EU legislation addressing/regulating the issue if exists
Access of the public to project's data, alternative solutions and environmental impact of the project Informing the public that they may have access to the EIS, so that they express their opinion The competent environmental Authority sends information and data to the Committee of the Region, so that they publicize it and inform the public, but the conduct of public debate procedure is not mandatory	a) Greek Law 2472/1997 & 3471/2006 for the protection of personal data b) Greek Law 2121/1993 concerning the copyrights c) Greek Law 1733/1987 concerning the protection of inventions and industrial design in d) Common Ministerial Decision 77921/1440/1995 concerning the access to environmental information.
There should be open access to the outcome of the Environmental Permitting Process, renewal or amendment of the Decision of the Environmental Approval: publication on the CL@RITY website.	a) Common Ministerial Decision No. 77921/1440/1995 on the free access of the pubic to Authorities concerning environmental information. b) Greek Law 3861/2010 for administrative decisions' publication on the CL@RITY website.

4.1.4 Italy

Data handled by the system and information flows related

Information type	**Category (PI,NPI /S, NS,HS)***	**Data Flow Category Mapping**
Applicant Name, Business Address, Communication Information, Address/Tel/Fax/e-mail	PI/S	From Firm/Owner to the Environment Ministry (D)
Generic registered user personal information	PI/S	A,B,C,D (even if not flowing, these information are retained by the system)
Application File with indication of the plant, the type, scope of its activities, and all the technical information and evaluation required by the electronic application; Revised Application File	NPI/HS	From Firm/Owner to the Environment Ministry (D)
Information on members of the IPPC commission nominated	PI/S	From Environment Ministry to IPPC Commission (B)
Information on the start date of the evaluation process	NPI/NS	From Firm/Owner to the wide public (D)
Extract of publication on newspapers	NPI/NS	From Environment Ministry to Firm/Owner (C)
Applicants File Check Results, Missing Documentations, Types of Missing Documents	NPI/HS	From IPPC Commission to the Environment Ministry and Firm/Owner (B, C)
Service Consultation Convening Notification Data	NPI/NS	From Environment Ministry to IPPC Commission, to Firm/Owner, to other Ministries and registered Stakeholders (B, C)
IPPC Commission Decision	NPI/HS	From IPPC Commission to the Environment Ministry (B)
Remarks on the application	NPI/NS	From any registered stakeholder to the Environment Ministry (B)
EIA Ordinance	NPI/NS	From Environment Ministry to Firm/Owner and to the wide public (C)
EIA Implementation start	NPI/NS	From Firm/Owner to the Environment Ministry (D)
Self-monitoring & control results	NPI/S	From Firm/Owner to the Environment Ministry (D)
Failure Report	NPI/HS	From Environmental Agency to Environment Ministry (B)
If during the field check any	NPI/S	From Judiciary Authority to the

Information type	**Category (PI,NPI /S, NS,HS)***	**Data Flow Category Mapping**
unpermitted/unlicensed activity is found, the judicial authority issues penalties according to legislation or order stop of activity		Firm/Owner (C)

Use cases vs Privacy Issues

Use case that can trigger the issue	**Transaction, stakeholders involved, data/information exchange**	**Privacy issue that can arise**	**National and/or EU legislation addressing/regulating the issue, if exists**
EIA_UC01_Applicant_Registration **MAH_UC01_Registration**	Registration of Applicant Personal/Company data in the system	Protection of personal data	Legislative Decree 196/2003 Legislative Decree 7 March 2005, n. 82
EIA_UC02_Application **MAH_UC02_Application** **MAH_UC04_ApplicationUpdate** **EIA_UC14_Counterarguments To Prescriptions** **EIA_UC20_SelfcheckDataUpdate** **MAH_UC06_UpdateForChanges**	Submission of the electronic application, or documents updating it	Providing information on the project (type, raw materials, industrial design, production line etc.). In case that data or information necessary for the EIA fall into restrictions of copyrights or protection of inventions and industrial design, they have to be marked as restricted in order to avoid diffusion to the wide public.	Legislative Decree 196/2003 Legislative Decree 7 March 2005, n. 82
EIA_UC12_AdviceInquiry Transmission **EIA_UC15_Arrangement CAI_MCP** **EIA_IPPC_UC21_InspectionExecution** **EIA_UC22**	Exchange of document containing sensitive data about the evaluation process	Third party access to information reserved before the conclusion of the assessment process	Legislative Decree 196/2003 Legislative Decree 7 March 2005, n. 82

Use case that can trigger the issue	Transaction, stakeholders involved, data/information exchange	Privacy issue that can arise	National and/or EU legislation addressing/regulating the issue, if exists
FailureReport **EIA_UC08_Assessment Preparation** **MAH_UC05_AdviceIssuing** **MAH_UC10_EIA-IPPC Suspension**			
EIA_UC06_WorkSpace Definition **MAH_UC03_ Validation And Appointment**	IPPC Commission members share application related data with other stakeholders	Confidential information to be protected against diffusion to non-authorized parties	Legislative Decree 196/2003 Legislative Decree 7 March 2005, n. 82
EIA_UC10_WorkspaceAccess **EIA_UC07_ Application Publication** **EIA_UC18_IPPCConsultation** **EIA_UC23_BrowseKnowledgeBase** **MAH_UC09 FormalSuspension**	Access to the public documents related to the application	All the information made public have to be accompanied by the agreement of the owner to make it public	Legislative Decree 196/2003 Legislative Decree 7 March 2005, n. 82
All	Any transaction	The cookies stored in a user's browser can allow tracking of the users activity on Internet	Legislative Decree no. 69/2012

4.1.5 Croatia

Data handled by the system and information flows related

Information type	**Category (PI,NPI /S, NS,HS)***	**Data Flow Category Mapping**
Investor personal data	PI	All categories possible in different phases of permitting process
Investment/project business sensitive data (location, technology details, size details,…)	S (it could be HS)	All categories possible
Env.Consultant analysis know-how (proprietary methodology, modelling system…)	S	All categories possible

Use cases vs Privacy Issues

Use case that can trigger the issue	**Transaction, stakeholders involved, data/information exchange**	**Privacy issue that can arise**	**National and/or EU legislation addressing/regulating the issue if exists**
Use case 2	As defined in use case (WP3)	As defined in D6.1 Cro-pilot (issue 2 and 3)	As defined in D6.1 Cro-pilot
All use cases	As defined in use case (WP3)	As defined in D6.1 Cro-pilot Issues related to pilot phase	As defined in D6.1 Cro-pilot Issues related to pilot phase

5 Guidance to the technical design

The technical design of the eEnviPer system has to be tailored in order to comply with all the requirements imposed by the relevant legislation and, in this regards, all the best practices diffused in IT environments for the insurance of confidentiality, availability, integrity of data – as all these aspects are strictly link to the data protection - have been considered.

A crucial aspect to be considered in this context, furthermore, is the wide scale deployment of cloud computing services, which can trigger a number of data protection risks, mainly a lack of 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 eEnviPer system in relation to data protection:

Minimization: eEnviPer system should only handle minimal data about users.

Transparency: the eEnviPer system 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 each user interface allowing 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 evaluation process, will not be allowed to submit the application. 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 environmental permitting 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 process for other 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 anonymised. 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 unauthorised tracking of the users' activities on the Internet.

Security: The protocol used for data exchange within eEnviper 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". eEnviPer system, 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 centres 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 if it is wise to require the cloud provider to equip the hosting of the eEnviPer service entirely within each single country in which it is delivered, and to ensure that the data does not go beyond the boundaries of that country.

6 The eEnviPer Technical Approach

The technical solution set-up for the eEnviPer framework has been designed taking into due consideration the recommendations drafted in this document and implemented in order to minimize its impact in terms of privacy and confidentiality of personal data.

This chapter illustrates the technical choices done with respect to this issue. Some additional development are envisaged before the operational launch of the platform, in order to fully accomplish with the recommendations defined in this document.

eEnviPer has been built on a platform based on open source technologies like PHP, Smarty, jQuery and ExtJS. eEnviPer's architecture design implements the model-view-controller (MVC) design pattern, which is a widely adopted architecture in Web applications. MVC aims to separate business logic from the user interface, so that changes in each part do not affect the other. In MVC, the model represents the information (the data) and the business rules; the view contains elements of the user interface such as text, form inputs; and the controller manages the communication between the model and the view.

The platform uses a number of security policies and rules to ensure the confidentiality, integrity and availability of electronic information captured, stored, maintained, and used by the eEnviPer platform. The eEnviPer framework, in fact, provides authentication mechanisms and policies to assure authorized access to the platform's data, the generation, maintenance and transmission of strong passwords. The security policies include:

- User Access Control mechanisms that provide the right privileges to the platform's users.
- System security mechanisms in order to protect data and eliminate risks as SQL injection, Cross-site scripting (XSS) and session hijacking.
- Secure protocols (SSL) and encryption mechanisms to allow the secure transmission of sensitive information over the network.

Furthermore, in a fully operational platform, DRAXIS will implement the eEnviPer platform with the electronic signature in compliance with EU Directive on Electronic Signatures 1999/93/EC. This action will provide further privacy and data protection regarding the platform submissions. E-signature processes can be supported through the integration of e-signature components that were developed during the Pan-European Public Procurement Online (PEPPOL [1]) project. Several contacts have been exchanged already with the involved PEPPOL partners in order to gain access to PEPPOL's components API and receive more technical information about this API. DRAXIS and PEPPOL designed a workflow explaining the eEnviPer project, the involved parties and how digital signing / validation processes will be integrated to the project's environmental permitting processes. After receiving the necessary feedback from PEPPOL's partners on

[1] http://www.peppol.eu/peppol-project

the above parts, our team performed an initial setup / configuration and internal testing of the components and the results proved that the integration target could be reached. Both teams have setup a schedule for developing, testing and deploying the full integration mechanism of the two tools within the next six-eight months, which will eventually result in an e-signature eEnviper module that can be integrated to any of the pilot platforms when necessary.

With respect to the cloud solution chosen, eEnviPer platform is hosted on the AppFog Cloud Platform and uses Amazon's Web Services (AWS) cloud infrastructure, which has been architected to be one of the most flexible and secure cloud computing environments available today. It provides an extremely scalable, highly reliable platform that enables users to deploy applications and data quickly and securely.

eEnviPer uses Amazon Simple Storage Service (Amazon S3) for storing the platform's data. Amazon S3 supports several mechanisms that provide flexibility to control who can access the platform's data as well as how, when, and where they can access it. Amazon S3 provides four different access control mechanisms: Identity and Access Management (IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication. Data can be securely uploaded/downloaded to Amazon S3 via the SSL encrypted endpoints using the HTTPS protocol. Amazon S3 also provides multiple options for encryption of data and supports logging of requests made against the Amazon S3 resources.

Finally, Amazon S3 complies with the EU data privacy regulations; customers, in fact, can choose to store all data in the EU by using the EU (Ireland) Amazon S3 Region, and this was the option chosen by eEnviPer.

7 Privacy Protection Issues in the Pilot Execution and Project Exploitation

The aspects to consider during the pilot execution with respect to privacy and data protection are the same identified as drivers for the system design.

Assumed that the test scenarios chosen for the pilot execution (or as demonstrations in the exploitation phase) are real environmental applications, the privacy issues that may arise are related to:

- access of the public to confidential data about the project and the company that submitted the application;
- restrictions of copyrights and (if necessary) protection of inventions and industrial design;
- exposure to 'Application File Information More Than Sufficient Levels', and 'Abuse of Information for Competitive Reasons';
- access of the public to personal sensitive data of the actors involved in the pilot execution (the applicant, the authorities representatives, the consultant involved in the evaluation process);
- confidentiality of the data exchanged during the assessment process before that the process completes;
- access to the outcome of the Environmental Permitting Process, renewal or amendment.

According to what reported by the project partners with respect to the pilot execution, no data has been published on the eEnviPer system that is not available otherwise, i.e. through traditional procedure.

An issue encountered was related to the investors not wanting their application details to be made public and environmental consultants not wanting their studies to be made available for download. With this respect, the set of laws related to Intellectual Property Rights protect copyrights of the environmental consultants for the databases and analysis generated and published within publicly available EIA studies. Confidential business data and information (including patents) are not required to be published in EIA study; nevertheless, they are protected by the laws. However, in Croatia the issues were resolved in testing phase by using permitting processes that had investor approvals for testing. For production use, this issue needs to be discussed and agreed with the national permitting authority, the Ministry of Environment and Nature Protection.

In order to protect the identity of users, citizens are enabled to anonymously inspect all available data, as they would be able to do if asked for the data in person.

Citizens, furthermore, can use the forms provided by eEnviPer to post comments during the phase when commenting is allowed by the public authority

In this regard, it has been evaluated the possibility that persons can post comments anonymously on the on-going environmental procedures, rather than being necessarily registered on the platform to be enabled to do it.

The pilot countries had a different approach towards this issue.

In Serbia, for instance, citizens can post comments even anonymously, because this is what is indicated by the local regulation.

In Italy, instead, only citizens registered on the system are enabled to post comments; the current procedure, in fact, asks them to be well identified, because they can be convened to the debates related to the authorization process on-going, and because otherwise public authorities and investor would not have any possibility to protect themselves against offences.

In Croatia, furthermore, a relevant number of citizens involved objected to give personal information (name, e-mail, phone) while making comments on particular application, so the platform was changed to enable anonymous citizen contributions.

eEnviPer, therefore, needed to find a balance between empowering citizens to express their opinion on environmental issues, but not allow itself to become a tool for exchange of insults or accusations. In the final solution implemented, the public authority responsible cannot reject any comments, information, analyses received through the system; however, citizens' comments are not visible to other members of the public before the public authority legal and ethical expert has checked them and authorised their publication. In this way, eEnviPer protects others involved in the procedure from possible defamation. However, any censorship of messages is tracked in the system, so that decisions can be justified on request of the users to avoid any misuse of power.

Finally, who participate in the service testing and evaluation can leave their comments about the service even without leaving any personal data.

8 Conclusion

As an e-government system that enables management of environmental permit processes, eEnviPer addresses certain ethical and legal issues and must comply with a number of European and national legal acts that regulate them. This document, in particular, deals with privacy and data protection, which are socio-technical issues to be considered in all the phases of the project, as they lead, in fact, to requirements for the design of the technical infrastructure, as well as for policies and agreements that have to be enforced on at organizational level.

Although the invasion of privacy is a problem that exists in offline systems as well, electronic environment brings an additional special dimension. Data managed by electronic systems, therefore, must be secure from viruses, hacker attacks, forgery, etc. This security means protection of information and information systems by ensuring confidentiality, availability, integrity, authentication, and non-repudiation. The cloud-computing environment, finally, adds a further degree of complexity to the global picture.

The following table summarizes the findings of the analysis reported within this document, describing how eEnviPer tackled the problems individuated, and which solutions have been identified for the project implementation and will be fully applied to the set-up of the operational system.

Table 2: Main findings on privacy impacts

Issue evaluated	eEnviPer solution
Nature of data managed	Environmental permission is a transparent process that involves processing of personal data in a limited measure. The eEnviPer system enables access to the same data that is otherwise available by in-person requests and through paper documents, and no data has been published on the eEnviPer system that is not available otherwise, i.e. through traditional procedure. Intellectual Property Rights protect copyrights of data generated in the context of an EIA application and published within publicly available EIA documents. The system, anyhow, adopts some basic practices that prevent any inadvertent or accidental failure on sensitive data handling. eEnviPer system, in fact, only handles **minimal** data about users, and keep personal data for no longer than is necessary for the purposes for which the data were collected, proceeding with their **erasure** if they are no longer necessary. Data collected are not automatically shared, but their publication happens just upon user notice.

Issue evaluated	eEnviPer solution
Data transmission	eEnviPer system collects personal data of the users just for the specified purposes of the environmental permitting process and, anyhow, in accordance with the requirements of **transparency**, informs data subjects about which data are stored, for which purpose they are retained, who these data will be transmitted to and for which purpose. In the case the user is asked to provide data potentially sensitive, the system asks the user's **consent** before transmitting them.
Authentication & Security	The platform provides **User Access Control** mechanisms that provide the right privileges to the platform users. Only authorized users can modify the data/information, whose **integrity**, **durability** and **accessibility** – for the persons granted with the proper permissions - is guaranteed by the eEnviPer solution, first, and by the cloud provider, then. The platform also provides additional security mechanisms in order to protect data and eliminate risks as SQL injection, cross-site scripting and session hijacking. Furthermore, the platform supports **secure protocols** (SSL) and **encryption** mechanisms to allow the secure transmission of sensitive information over the network.
Accountability	The system makes possible to establish what an entity did at a certain point in time in the past and how. This way, no one that participated in the process can **repudiate** the provided data/information (if users submit comments, e.g. they cannot later say that they did not do it).
Data hosting	eEnviPer stores the platform data using the Amazon Simple Storage Service (Amazon S3), which has been evaluated one of the most flexible and **secure cloud computing environments** available today. In compliance with the EU data privacy regulations, eEnviPer exploited the possibility offered by the Amazon S3 solution to **store all the platform data within the EU boundaries**.

Issue evaluated	eEnviPer solution
Citizen Participation	eEnviPer allows **anonymity** of users. This concept applies not only at system level (data consultation is enabled for anonymous users and some pilot implementation enable users to post comments without being registered and authenticated), but also at organizational level (evaluation forms have been collected, either on-line or on paper, giving users the option to stay anonymous). The system, furthermore, does not stores **cookies** on the users' computers in order to prevent any unauthorised tracking of the users' activities on the Internet. However, anonymity opens the possibility for using the participatory system for **defamation**. To avoid this problem, eEnviPer makes the comments visible only after they have been approved by the relevant person within the public authority.

References

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

[2] 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.

[3] 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.

[4] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF)

[5] 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)

[6] Directive 2000/31/EC of 8 June 2000 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:NOT) on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L 178, 17/7/2000 p. 1-16; this directive replaces Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L 024, 30/1/1998 p. 1-8.

[7] INDUSTRY RECOMMENDATIONS TO VICE PRESIDENT NEELIE KROES ON THE ORIENTATION OF A EUROPEAN CLOUD COMPUTING STRATEGY, November 2011

[8] 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

[9] 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

[10] 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.

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

[12] Geodata.gov.gr-Public data, Open data website, Terms of use–Policy of personal data protection. http://www.geodata.gov.gr

[13] Greek Law 2472/1997 (Governmental Gazette Vol. A/50/10.04.1997) "Protection of the individual against processing of personal data".

[14] Greek Law 3471/2006 (Governmental Gazette Vol. A/133/28.06.2006) "Protection of personal data and privacy in the electronic communications sector and amendment of Law 2472/1997".

[15] Greek Law 3979/2011 (Governmental Gazette Vol. A/138/16.06.2011) "On e-Government and other issues" which regulates the use of information and communication technology by the public organizations and institutions for their transaction within the public sector and between the public sector and the private one.

[16] Ministry of Administrative Reform and e-Government of Greece, website http://www.ydmed.gov.gr/

[17] 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.

[18] Region of Crete website, Terms and conditions of use, http://www.crete.gov.gr

A. Annex A – Privacy Checklist

Hereafter is reported a privacy checklist, 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 eEnviPer system 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?
- Does the web platform and/or the organisation share, transfer, or release any information to third parties?
- Does the web platform contain links to other websites?

- Are 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 organisation?
- 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 organisation?
- Is sensitive information differentiated from less sensitive information, and is there any access restriction applied according to this categorisation?
- 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?