Deliverable D1.32

Privacy requirements and personal data legislation - second iteration

Project Acronym	OASIS
Grant Agreement number	297210
Project Title	Towards a cloud of public services

Project co-funded by the European Commission within the ICT Policy Support Programme

Deliverable reference number and title	OASIS_D1.32v0.4
Status	Final

Dissemination level[1]	PU	**Due delivery date (project month)**	M24
Nature[2]	R	**Actual delivery date**	14/02/2014

Lead beneficiary	UBRUN
Contributing beneficiaries	All pilot sites
Author(s)	Uthayasankar Sivarajah, Bruno Thuillier, Huseyin Ozgur Unsal, Lacho Mateev, Massimo Massimino, Alfons Bataller.

Revision History

Revision	Date	Author and Organisation	Description[3]
0.1	10/09/2013	Uthayasankar Sivarajah, UBRUN	Creation of first draft
0.2	14/01/2014	Uthayasankar Sivarajah, UBRUN	Revised version addressing comments from WP1 Leader and Pilot Sites.
0.3	20/01/2014	Uthayasankar Sivarajah, UBRUN	Revised version addressing comments from WP1 Leader and Pilot Sites.
0.4	14/02/2014	Uthayasankar Sivarajah, UBRUN	Final version

[1] Dissemination level: **PU** = Public, **CO** = Confidential, only for members of the consortium and Commission services

[2] Nature of the deliverable: **R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

[3] Creation, modification, revision, final version for evaluation, revised version following evaluation

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise.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

Deliverable abstract

This deliverable's main objective is to provide an analysis of the changes to the already presented information and recommendations on privacy issues and guidelines for both the OASIS platform and its services since the submission of D1.31. As the initial analysis which formed part of deliverable 1.31 was presented at an early stage, it was important for this deliverable to re-examine the developments of the OASIS platform and the services offered by it to present a more developed privacy requirements analysis. To do so, any changes on the data protection rules and guidelines across the European Union and the national legislations of the pilot sites of OASIS were examined and reported. Afterwards, the OASIS architecture and its operation in the cloud are analysed in detail to report any privacy and security issues taking into account of the latest national data protection context of the pilot sites. The main findings of this deliverable are that a) the amendments to the national legislations has had no major implications on the OASIS services b) the OASIS modules such as data core, social graph and authentication have been identified as the key elements presenting some privacy concerns c) most of the public services still process data that are not sensitive personal data and hence low risk for information privacy exists. This deliverable has therefore reported a detailed privacy analysis of the OASIS architecture and its services and reported guidelines to address the presented privacy issues.

Project Management Review

	Reviewer 1: WP leader			Reviewer 2: B. Thuillier		
	Answer	**Comments**	**Type***	**Answer**	**Comments**	**Type***
1. Is the deliverable in accordance with						
(i) the Description of Work and the objectives of the project?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) the international State of the Art?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
2. Is the quality of the deliverable in a status						
(i) that allows to send it to European Commission?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) that needs improvement of the writing by the originator of the deliverable?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(iii) that needs further work by the partners responsible for the deliverable?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a

* Type of comments: M = Major comment; m = minor comment; a = advice

Table of Contents

1. Introduction

This deliverable is the result of the Task 1.3 of Work Package 1 and it is the second iteration of the previously submitted deliverable 1.31, the report on the legislations in each country and the preliminary privacy requirements for the OASIS services. This report's main objective is to provide an analysis of the changes to the presented information and recommendations on privacy issues and guidelines for both the OASIS platform and the services offered by it since the submission of D1.31 in January 2013. As the initial analysis which formed part of deliverable 1.31 was presented at an early stage, it was now important to address the developments in the services and to present a more developed and comprehensive analysis of the OASIS architecture.

Firstly, any reported change on the national legislation of each of the five pilot site countries are presented by focusing on the amendments made to the legislations since January 2013. Second, the OASIS architecture and it's operation in a cloud environment is examined in detail to report privacy and security issues according to the latest national data protection context of the pilot sites. In doing so, providing a comprehensive privacy analysis of the OASIS architecture and its use of cloud computing. Third, the changes to the services deployed in OASIS platform are reported providing additional information reported in terms of service description and personal data processed by these services. Afterwards, the services provided by the OASIS in each pilot site are re-examined considering especially as they are going to be deployed in several countries and what legislative requirements exist to them, the type of data processed from the applications and any additional security and privacy requirements that might be required.

Finally, an analysis on the privacy and security guidelines to the design and deployment of high-risk services in OASIS is presented. This was presented mainly because although the services selected for OASIS seem to be of low-risk for privacy requirements and personal data, the main aim of OASIS is to be able to cope with the provision of low to high risk services.

2. Data Protection in Europe

2.1. Changes on relevant legislations

There have been no reported changes to European Data Protection Directive 95/46/EC and E-Privacy Directive 2002/68/EC since the submission of D1.3.1 in January 2013. The proposed comprehensive reform of the Directive 95/46/EC to strengthen online privacy rights and boost Europe's digital economy has also still not been enforced by the European Commission. Therefore section 2 in D1.31 and the changes below will be the main reference point for this deliverable.

3. Personal data protection legislation at the Pilot Sites

This section reports any changes to the personal data legislations at the national level for each pilot site.

3.1. Personal data legislation at Pilot Site 1: France

3.1.1. Changes on relevant legislations

In France, there have been reported changes to the personal data legislations since the submission of D1.3.1. Table 1 highlights which of the legislations has reported a change.

Personal data legislation: France	
Stated Legislations in D1.31	*Changes*
Digital and Privacy Law	Yes
Electronic Exchange Legislation	No
Supervisory Authority	No

Table 1: Changes to Personal data legislation in France

The subsequent sections present detailed explanation of the changes highlighted in Table 1.

3.1.1.1. Digital and Privacy Law

The French legislation evolved with a decree made on July 4th, 2013, authorizing under conditions, the implementation of automated **processing of personal data**. The purpose of this was to provide users with one or more on-line public services. The conditions of the decree were as follows:

Article 1:

Public authorities, EPCIs (public inter-municipality cooperation establishments), joint associations, local public establishments and groupings of public interest, local public companies they are members of can implement **personal data processing** whose objective consists in making one or more e-administration services available to the users in the conditions set out in this Order.

These tele-services enable the users to complete administrative procedures with the administrative bodies mentioned in the preceding paragraph. It is for their agents to ensure the processing and follow-up.

The tele-services concerned can manage the procedures which are part of the following fields:

1. Taxation	Tax or household refuse collection tax. Tourist tax
2. Labour and social	Job-fair. Apprenticeship. Professional training. Traineeship, job application. Management of social welfare (demand, allocation and follow-up) in the following fields : - application for housing and/or assistance ; - grant ; - independence social allowance ; - assistance to disabled persons ; - active solidarity income
3. Health	Child and maternal protection Vaccination plan Heat-wave plan Emergency Action plan Applications for registration as a child minder
4. Transport	Registration, follow-up and online payment of local or academic services, individual or public transport (bicycle, car, bus, etc.). Information on traffic conditions
5. Civil status and citizenship	Applications for extracts or copies of civil status records, family book. Compulsory registration for the Defence and Citizenship Day/ citizen census. Registration on electoral lists. Notification of address changes. Proof of accommodation. Authorization to leave French territory. Application for identity and travel documents or residence permits.
6. Relationships with the elected representatives	Municipal communication. Relationships between the users and the elected representatives (demand of appointment, etc.).
7. Curricular and co-curricular activities, sport and sociocultural activities	Case management (registration, follow-up and online payment) in the following fields : - leisure centres ; - touristic activities ; - holiday centres ; - schools ; - crèches and nurseries ; - school catering ; - sports activities (swimming pool, sports hall, etc.) ; - sociocultural activities (library, media library, museum,

	local room booking) ; - hiring of local room or equipment ; - home-delivered meals.
8. Economy and town planning	Recording of the activity in the socio-economic directory. Assistance to companies. Request for professional premises ; Case management (application, allocation, follow-up and online payment) in the following fields : - water-sanitation; - building permit; - land-use planning permit; - demolition permit; - planning certificate; Declaration of : - completion of works - construction site opening ; - intent to waive.
9. Specific policies and roads	Temporary authorisation for a licensed public house. Declaration of dogs of first or second category. Certificate of change of residence. Payment, subscription or parking permit Market/fair location. Access to pedestrian areas. Lost items. Reporting of pollution in terms of noise, odours and view. Request for intervention on the public field (maintenance of green areas, public lighting, containers, etc.). Cemeteries (allocation of cemetery plots). Filmmaking.
10. Relationships with the users	Relationships of the users with the services (demands for appointments, etc.) Registration to the ceremony given in honour of new residents. Exercise of Information Technology and Data Protection rights (information, modification, deletion request, etc.).

Table 2: Tele-Services listed in Article 1

Any public service of the same activity field and having the same categories of data than one of the tele-services listed previously is included in the scope of that order.

Article 2:

When the authorities mentioned in the first article implement or take part in an access portal, in a tele-services package, the device guarantees the protection of data between the fields mentioned in the first article for the services and prohibits the creation by the administrative authority of a population file and a unique identifier for the users.

Without prejudice to the previous paragraph and the legal and regulatory provisions in force, in order not to ask the user for information or data he would have already given to a service and which would be necessary to the processing of an administrative task by another service; the latter can, once having received the express non equivocal agreement of the user, obtain these information or data from the contact service detaining them.

Article 3:

Categories of personal data stored are the following:

1. For the management of the access to tele-services, according to the identification level required by these tele-services :

- personal login chosen by the user;
- password chosen by the user;
- the user mobile phone if he chooses this access mode ;
- information contained in the 'daily life card' of the user ;
- the electronic certificate of the user if he chooses this access mode ;
- if applicable the federation keys or alias generated by the system enabling the user to create links with his various accounts.

2. For the successful completion of the administrative procedures :

- the personal information and data strictly necessary to the implementation of the administrative procedures mentioned in the first article.

When, for the implementation of an online administrative procedure, the **processing of sensitive data**, under article 8 of the 6 January 1978 above-mentioned law, is made necessary by a legal or regulatory text or has been expressly and unequivocally approved by the user, the confidentiality of these data is particularly reinforced by additional technical safety measures. These reinforced safety measures are also implemented for all data benefiting from particular protection under the law of 6 January 1978, such as the persons' registration number to the national directory of identification of natural persons or those mentioned in article 9 of the above law. The list of personal data recorded and the information mentioned in article 32 of the 6 January 1978 law are made available from the tele-services created under article 1.

Article 4:

The data storage periods necessary to the implementation of the administrative procedures and collected within the processings mentioned in the first article are the following:

- if the authority mentioned in article 1 implements or participates to a portal offering a tele-services package and if these data are sent to the relevant authorities of the administrative bodies mentioned in article 1, the data are stored by the portal for a maximum of three months. After this time period, they are deleted immediately ;
- in the other cases, the storage duration of data is related to the proper objective of each tele-service.

Article 5:

The recipients or categories of recipients of the data recorded by the processing are the only authorities lawfully entitled to know and to handle the administrative procedures of the tele-service users.

Article 6:

Tele-services subject matter of this article are implemented according to the provisions of Article 34 of the 6 January 1978 above-mentioned law, articles 4 and 9 of the 8 December 2005 above-mentioned order and articles 3 and 5 of the 2 February 2010 above-mentioned decree. So the administrative authorities mentioned in the first article must, before the implementation of any tele-service, make a risk analysis taking into account the respect of the users private life.

Article 7:

The implementation of the processings mentioned in article 1 shall be subject to prior sending to the National Commission for Data Protection and Liberties, under III of Article 27 of the 6 January

1978 above mentioned law, of a statement referring to the present order. This statement of 'conformity to a unique regulatory act' is made online on the CNIL website.

However this statement does not cover the implementation of processings of personal data related to processings mentioned in article 1, which remains submitted to the implementation of preliminary formalities planned in chapter IV of the 6 January 1978 above-mentioned law.

Article 8:

Access, modification and deletion rights mentioned in articles 39 and following of the 6 January 1978 law shall be exercised with the person in charge of tele-service according to the modalities published on the tele-service website. The right to opposition is given effect through the continuation of an alternative to tele-service giving the possibility to access in the same conditions to the same public service supply than the one offered by the said tele-service.

Article 9:

The general secretary for the modernisation of public action and the general manager of public authorities are in charge, within their respective areas of responsibility, of the implementation of this order which shall be published in the Official Journal of the French Republic.

3.1.2. Impact of the changes of the legislation to the pilot site

The latest amendments to the personal data legislation in France mentioned above have had some implications on the privacy guidelines for the pilot. The key change evident from the decree is that it allows the administrative bodies listed in Article 1 to process personal data where the objective is to make one or more e-administration services available to users. However, it is highlighted in Article 2 that when the authorities mentioned in Article 1 implement or take part in an access portal such as OASIS, the public authority need to ensure that the user is not requested for information or data he/she would have already given to a service and which would be necessary to the processing of an administrative task by another service.

The changes that the pilot site has to be aware of from the latest amendments have been summarised below:

- **Exchange of personal data:** In article 2, the decree aims at defining the type of tele-service that **must not communicate with each other**. For instance, a request made for citizen data for school registration (Pack 7 in article 1) cannot be used together to identify the personal details with another a request of professional training (Pack 2 in article 1). In other words, the citizen data from Pack 7 (e.g. name, address) and Pack 2 (e.g. name, age, and occupation) cannot be used together to identify the full personal details (e.g. name, address, age, and occupation) of a user.
- **Processing of sensitive data:** In article 3, it is highlighted that when implementing an online administrative procedure, the processing of sensitive data (e.g. Pack 3 – Health data)**,** is made necessary by a legal or regulatory text or has been expressly and unequivocally approved by the user. Additionally, the confidentiality of these data needs to be reinforced by technical safety measures such as the persons' registration number to the national directory of identification of natural persons.
- **Handling of data:** In article 5, it is highlighted that only the lawful authorities in charge of the administrative procedures of a tele-service is entitled to process and handle data of the user.
- **Storage of data:** In article 4, it is highlighted that the authority need to ensure that the data stored by the portal can only remain for a maximum of three months after which it has to be

deleted immediately. In other cases the storage duration of data is related to the proper objective of each tele-service.

- **Performing a risk analysis:** In article 6, it is highlighted that it is a must for the authorities listed in article 1 to perform a risk analysis of the user (taking into account of the users private life) prior to the implementation of any tele-service.

It is therefore important for the pilot site based in France to be aware of these changes when providing e-administration services through the OASIS platform.

3.2. Personal data legislation at Pilot Site 2: Italy

There have been no reported changes to Personal data legislation in Italy since the submission of D1.3.1. However, it is to be noted that **Comune di Bussoleno** is no longer a pilot site for OASIS and therefore there will be only **one pilot site (i.e.Turin Province) based in Italy**.

3.3. Personal data legislation at Pilot Site 3: Bulgaria

There have been no reported changes to Personal data legislation in Bulgaria since the submission of D1.3.1.

3.4. Personal data legislation at Pilot Site 4: Turkey

3.4.1. Changes on relevant legislations

In Turkey, there have been reported changes to changes to the personal data legislations since the submission of D1.3.1. Table 2 highlights which of the legislations has reported a change.

Personal data legislation: Turkey	
Stated Legislations in D1.31	*Changes*
Turkish Constitution	No
Regulation on Personal Data Processing and Protection at Telecommunication Sector	Yes
The Draft Law on the Protection of Personal Data	No
Civil Code	No
Criminal Code	No
Labour Code	No
Banking Law and The Law on Debit & Credit Cards	No
Health related Legislation concerning Sensitive Data	No
Supervisory Authority	No

Table 3: Changes to Personal data legislation in Turkey

It is also to be noted that there have been no changes made to the Turkish Constitution with regards to Data Protection yet; however there is an undergoing debate on introducing an amendment, much stronger as compared to the existing provisions.

The subsequent sections present detailed explanation of the changes presented in Table 2.

3.4.1.1. Regulation on Personal Data Processing and Protection at Telecommunication Sector:

A set of changes have been made by an amendment on 11.07.2013. Below are the substantial changes introduced by the amendment.

Article 2: Following paragraphs replaces the previous versions.

1. Anonymisation: Rendering personal data unassociated with a specific or identifiable natural or legal person or its source untraceable
2. Unrealized call: Inoccurrence of communication despite the connection is established successfully
3. Operation log: Electronic records that contain at least the information related to the operation and its details, agent of the operation, date and time of the operation, and the point of connection of the agent, with a view to ensure identification of that operation at a future date by the persons accessing personal data
4. NAT: Technology enabling multiple subscribers to use a common IP through using of port information coming along with the IP address at the IP packs transmitted through the network

Article 4: Following paragraphs have been added.

1. Personal data cannot be transferred out of the country.
2. The limits of the consent given by the subscriber as to processing of the personal data includes the processing by the third parties authorized by the Service Provider, provided that the authorization is exclusive to the service.
3. Service Provider is held liable for ensuring the confidentiality of private data, security and due use of it, including prevention of violation of the provisions of this Regulation by the third parties authorized by the operator.

Article 5: *Following paragraphs replace their previous versions.*

1. Service Providers are responsible to ensure private data can be accessible only by the authorized people, and security of systems that are used to store private data and the applications used in accessing private data.
2. Service Providers are responsible to keep the logs of instances of accessing private data and other systems associated thereof.
3. The Authority is in capacity to request from the Service Provider to disclose all the information and hand over all the documents regarding the systems where private data is stored and the security measures in effect.

Article 13:

The below paragraph replaces the previous version of the second sub-paragraph of the clause “c” of the first paragraph the Article 13.

1. In reference to access to the internet, electronic mail and internet telephone, date and time of starting and ending of session as of access to the internet, assigned dynamic or static IP address, port information in addition to the IP address for NAT used networks, subscriber/user ID, date and time of opening and ending electronic mail or internet telephone session

Article 14 changed as follows:

Duration of Keeping Data by the Service Providers

1. Data categorised in Article 13 should be kept for one year upon the realization of communication, whereas logs of unrealized calls shall be kept for three months.
2. Private Data in question as to an investigation, examination, inspection or dispute shall be kept until the completion of such practise or the end of such situation.
3. Logs of instances of accesses to private data and other systems related thereof shall be kept for a period of four years.

Article 15:

Clause “b” and “d” of the first paragraph of the Article 15 is replaced with the following:

- b) Storing of data within the country
- d) Termination or anonymisation of processed or stored data within a month at the most after the end of the end of the duration of its storing, or systematic or report-based logging of such operations

The Law 5651 on Regulation of Internet based Content and Counteraction against the Crime that is committed via such Content.

Content Providers’ responsibility

Article 4

(1) Every content provider is liable for the compliance of the content it put to use online. Content provider shall not be held liable for the compliance of the content, which belongs to others and it establishes a linkage to; however it shall indeed be liable pursuant to the general provisions of this law, on the condition that it is explicit from the way of provision that it endorses the content and provides access to the content willingly.

Article 5

(1) Hosting service provider shall not be held liable for the compliance of the content, which it hosts.

(2) Without prejudice to the provisions regarding the penal liability for the illicit content it hosts, hosting service provider is under the obligation to remove the content which does not comply with the legal provisions, upon being reported pursuant to the Articles 8 and 9, and provided that it is technically viable.

Decision on interruption of access and execution of such decision

Article 8

(1) Access to the online content about which there is sufficient consideration that it suits to one of the criminal acts listed below.

a) Criminal acts outlined in the Turkish Criminal Code 5237 and dated 26.9.2004;

1) Driving someone to suicide;
2) Abusing minors;
3) Drug abuse and enabling drug abuse;
4) Hazardous substance provision for the sake of health concerns;
5) Obscenity;
6) Prostitution;
7) Providing premises and allowing for gambling

3.4.2. Impact of the changes of the legislation to the pilot site

The latest amendment to the personal data legislation in Turkey mentioned above does not have direct implications on the privacy guidelines for the pilot site. The key point about the Regulation (The Directive on Processing of Personal Data and Protection of Confidentiality at the Electronic Communications Sector) is that it does not concern organisations providing online services. In the Turkish Regulation, "Service Provider" refers to a company which renders electronic communications services within the framework of authorization and/or provides electronic communications network and operates the infrastructure thereof; or in other words telecom companies providing access to internet (i.e. broadband) based on subscription. As a result the Turkey pilot site does not yet have any legislation that governs the dealings of service providers such as the pilot site.

The latest changes to the Turkey legislations have been summarised below:

- **Transfer of personal data:** In article 4, it is stated that ***personal data cannot be transferred out of country***, so there is a strict need to ensure that the personal data of users remains in Turkey.
- **Handling of data:** In article 4, it is reported that the ***service provider is held liable*** for ensuring the confidentiality of private data, security and due use of it, including prevention of violation of the provisions of this Regulation by the third parties authorized by the operator. In addition the changes in article 5, requires the service provider to ensure that only authorized people have access to private data and see to that there is tight security systems in place to store and allow applications to access private data.
- **Traceability/Logs of data:** In article 2 it is highlighted that there is a need *to* ***maintain an operation log*****,** i.e. electronic records that contain at least the information related to the operation and its details, agent of the operation, date and time of the operation, and the point of connection of the agent, with a view to ensure identification of that operation at a future date by the persons accessing personal data.
  Furthermore, in article 5, it is highlighted that service providers are responsible to keep the logs of instances of accessing private data and other systems associated thereof. In addition, the authority is in capacity to request from the service provider to disclose all the information and hand over all the documents regarding the systems where private data is stored and the security measures in effect.
- **Storage of data:** In article 14, it is highlighted that Data categorised in Article 13 should be kept for one year upon the realization of communication, whereas logs of unrealized calls shall be kept for three months.
  Additionally, the change in the article 15 requires ***the termination or anonymisation of processed or stored data*** within a month at the most after the end of the duration of its storing, or systematic or report-based logging of such operations.

In addition, the Law 5651 stipulates the Content Provider to comply with general rules in reference to Criminal Code. However, it places the responsibility on the Content Provider rather than the hosting side. But once the Hosting Service Provider is reported about an illicit content, it may be held responsible for removing it. EMDA shall produce a Disclaimer stating that Service Providers should commit themselves to comply with such provisions.

It is therefore important for the EDMA to be aware of these changes when providing e-administration services through the OASIS platform.

3.5. Personal data legislation at Pilot Site 5: Spain

Catalonia of Spain has been introduced as a new pilot site since the exit of Comune di Bussoleno from Italy. Therefore, personal data national legislations of Spain has been now presented below which did not exist in D1.31.

In Spain, there is a legal framework for the Protection of Personal Data. The framework is comprised mainly by a central Act (REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal). All the public bodies must follow this legal framework in the implementation of the online public services. Additional security and privacy issues are included within the Legal Framework for the implementation of online public services. It is comprised mainly by the Act on Citizen electronic access to Public Services, the Royal Decree for the Implementation of the National Security Framework and the Royal Decree for the Implementation of the National Interoperability Schema. Blau Advisors will follow the above regulations and guidelines and will work closely with Brunel University to ensure full compliance in all areas.

The main elements for ensuring that the service will be developed according to the law are that in the moment of starting the service provision the public body must:

- Obtain the explicit authorisation of the citizen to share personal data with other Public Bodies with the purpose of managing the citizen request made
- Obtain the explicit authorisation of the citizen to retrieve personal data from other Public Bodies with the purpose of validating and verifying the personal situation according to the citizen request made

The information security is a relevant issue in the eGovernment legislation, as demonstrated in the Law 11/2007, of 22th June, on Electronic Access to Public Services. This recognizes the right of citizens to interact with public administrations by electronic means. In this sense, the concept of information security is reflected in the article 1.2, dedicated to the purpose of the rule that states that public authorities should use information technology in accordance with the provisions of this law according to ensuring the access, integrity, authenticity, confidentiality and preservation of data, information and the managed services in the exercise of its functions.

Article 4 of Law 11/2007 establishes the legal principles applicable to electronic administration, explicitly dealing into several principles related to the concept of security, corresponding to the following:

- Principle of protection of personal data, which is reflected in the respect to this fundamental right under the terms established by the Organic Law 15 /1999 on the Protection of Personal Data, as well as the right to honour and personal and family privacy .
- Principle of accessibility through systems able to use the services safely and especially to ensure universal accessibility and design for all the supports, channels and settings so that everyone can exercise their rights on an level playing field.
- Principle of security in the implementation and use of electronic media by the public bodies, under which at least the same level of assurance and security for the use of electronic media in administrative activity is required.
- The principle of proportionality, whereby only the guarantees and adequate safety measures are to the nature and circumstances of the various procedures and actions.

Article 6 of Law 11/2007 recognizes the rights of true citizens regarding safety such as:

- The right to guarantee the security and confidentiality of the information contained in files, systems and applications of Public Bodies (important in relation to the citizen right of conservation by public authorities of electronic data)

- The right to obtain identification measures so physical persons are able to use any electronic signature system for communicate with any public body.
- The right to use other allowed electronic signature system in the field of Public Bodies.

To ensure the effectiveness of these principles and rights, through the National Security Framework, approved by Royal Decree 3/2010 of 8 January, the security policy on the use of electronic media is established and it defines basic principles and the minimum requirements to allow an adequate protection of information.

This is addressed to Public Bodies, including The General Administration of the State, Authorities of the autonomous communities, entities comprising the local administration and the public entities that are linked to the previous ones.

The scope of the Schema lies in the regulation of basic issues for the use of information technology in three fields correspondent to administrative activity, the relations between public authorities (or internal activity, such as data transactions using interoperable networks) and the relationship between citizens and government (and in particular, the administrative procedures and electronic participation).

To ensure its compliance a set of measures are required to be implemented using a methodology that considers the main steps listed above:

- Establishment of a security policy
- Identification of the affected systems
- Determine the risk of affected systems
- Categorize the affected systems
- Implement the controls that apply

Law 11/2007 also pays special attention to cooperation between public authorities to ensure the interoperability of systems and solutions used in providing joint services to citizens and motivate the data transmission between the authorities and give citizens the right to choose between different channels to interact with government.

3.6. Conclusions

It is clearly evident from the above analysis that the personal data legislations in two pilot sites have had amendments since the submission of D1.31 and the inclusion of the national legislations for the new pilot site in Spain. This section has reported these revisions as it is important to be aware of the amendments to understand and keep up-to-date with the different national rules that govern the protection of personal information in these pilot sites. In doing so, this section has addressed one of the main objectives of this deliverable which is to ensure that the national requirements for information privacy are taken into careful consideration. As the data processed by the services will be handled under different legislative contexts, it is significant to identify and report any additional security and privacy countermeasures that may be required. Table 3 presents the main changes to the personal data legislations to the four counties, following the description of the national information privacy rules presented in this section.

Pilot Site	**Key changes to personal data legislations**
France	Digital and Privacy Law • Exchange of personal data • Processing of sensitive data • Handling of data • Storage of data • Performing a risk analysis

<table>
<tr><td></td><td></td></tr>
<tr><td>Bulgaria</td><td>No Reported Changes</td></tr>
<tr><td>Italy</td><td>No Reported Changes</td></tr>
<tr><td>Turkey</td><td>Regulation on Personal Data Processing and Protection at Telecommunication Sector
Transfer of personal data
Handling of data
Traceability/Logs of data
Storage of data</td></tr>
<tr><td>Spain</td><td>As the Spanish pilot site has been newly introduced, there was no national legislation information reported in the first iteration. The following table included here provides the information about Information Privacy Dimensions for the Spanish pilot site:

<table>
<tr><th rowspan="2">Dimension</th><th>Pilot Site</th></tr>
<tr><th>Catalonia</th></tr>
<tr><td>Personal data legislation in force</td><td>√</td></tr>
<tr><td>Compliance to the Directive 95/46/EC</td><td>√</td></tr>
<tr><td>Personal data definition</td><td>√</td></tr>
<tr><td>Obligation to install security measures proportionate to risks</td><td>√</td></tr>
<tr><td>Supervisory authority in force</td><td>√</td></tr>
</table>
</td></tr>
</table>

Table 4: Key changes to personal data legislations across the Pilot Sites

4. OASIS in the Cloud - Overview and Privacy Analysis

OASIS is based on Cloud Computing technologies that allows for an efficient access to the platform from any Internet access, to monitor and to manage the required resources. As reported in Deliverable D1.2, the OASIS ecosystem provides solutions in SAAS (Software as a Service) mode for users. Each module of OASIS and each federated application relies on a private cloud, and on a single hosting where there is no need for elastic hosting.

From the functional point of view of this architecture, OASIS is hosted on an IAAS (Infrastructure as a Service) platform in order to provide users a SAAS paradigm/model. A detailed schematic diagram that illustrates how OASIS works on the cloud platform is presented in D1.2b section 5.1.4. In sum, OASIS operates over a private cloud, implemented in two datacentres, and virtually extended via Internet.

OASIS will be hosted on a private cloud, provided by IPgarde based in France. IPgarde uses its own infrastructure, hosted in data centers that are located in France, managed by its own engineers based in Valence (France). IPgarde provides OASIS a private cloud in IAAS mode.

IPGarde has its own technical infrastructure, including:

- More than 450 physical servers
- 12 SAN for more than 150 To of data
- 30 42U bays
- a backbone with a capacity of 40 Gbps

Computer, networks and telecommunications equipment's are present in 4 data centers:

- Paris
- Lyon
- Geneva
- Bonneville (with dark fiber to Geneva)

OASIS cloud infrastructure is a virtualized infrastructure, in the two data centers of Lyon end Bonneville (in Rhone Alpes, France).

IPgarde uses 7 transit operators to ensure the best connection to Internet of its facilities in all circumstances:

- Level3
- Interoute
- 9Telecom - SFR
- Cogent
- GlobalCrossing
- Highwinds
- Telecom Italia

In the case of security and privacy issues for OASIS, some of the key elements of cloud computing such as virtualization, multi-tenancy, and outsourcing raise many questions for OASIS according to how its provider (i.e. IPgarde) runs their security policy and how they handle security issues as well as the responsibilities of the user [1]. By adopting Kronabeter and Fenz's [1] evaluation framework, a set of general security and privacy considerations as well as for legal and organisational requirements according to the EU data protection regulation has been presented below for the OASIS manager (i.e. Pole Numerique). These requirements are to be taken into account when Pole Numerique finalise the contractual agreement with the cloud provider.

4.1. Legal and organisational requirements:

These requirements cover governance, service level agreements, support and information, and compliance.

1. *Governance* includes the accountability, responsibility and transparency of an organisation. To fulfil these requirements, certifications and audits are used. Certifications and audits on which users can rely on are important since users are not able to get a complete insight of all security relevant issues. Hence, the provider should provide information about certification such as PCI DSS, ISO / IEC 27001, etc. and audit standards like SAS70 Type II. Third party audits should be a vital part of any assurance program.

2. *Service Level Agreements (SLAs)* are a contract between a provider and a user on the level of the provided service. SLAs and Terms of Service are essential to a reliable cloud provider. Service Level Agreements should contain:
    - Adequate system availability (uptime, response time)
    - Credits in case of outages
    - Adequate compensation for a breach
    - Notification in cases of failure or critical situations

3. *Support and Information* should be made available in a transparent and easily accessible way by the provider. The user should get as much information as possible. Therefore support and documentation by the provider is necessary. The following points should be made available:
    - Frequently Ask Questions (FAQ)
    - Help Lines and Wikis
    - Reaction time on requests
    - An extensive documentation about security
    - Information about the billing system and the business continuity strategy

4. *Compliance to laws and regulations* is the base of every service provider to become reliable. It refers to the organisation's responsibility to comply with regulations, laws and standards to assure secure services. With Audits it can be shown that a standard of security is reached but contractual obligations to protect personal information are essential for security and privacy issues. Laws and regulations can change depending on where the data is stored and processed. Legislative obligations (excerpt):

    - Health Insurance Portability and Accountability Act (HIPPA)
    - Gramm-Leach-Bliley Act (GLBA)
    - Federal Information Security Management Act (FISMA)
    - Sarbanes Oxley Act (SOX)
    - Safe Harbor
    - EU Data Protection Directive 95/46/EC

4.2. Data Protection requirements:

The protection of data is a vital issue to make a cloud environment secure. Therefore OASIS service provider should possess the following points to fulfil data and information protection requirements:

5. *Data Center:* A high standard of protection requires the access to information about data centers and the mechanism that are used to secure a data center. The following points about data centers should be considered:

    - Quantity - provide information about how many data centers are used to store and process data.
    - Physical Security - Information about the physical provisions to secure the data centers should exist.
    - Data Backup and Data Redundancy - It should be possible to backup and store data in several locations. The user should get information regarding backup procedures.
    - Information about the location of the data centers should be provided. In the best case the user can choose where the data will be stored and processed.
    - Data loss - The case of data loss should be stated in a contract, SLA or terms of service.
    - Data isolation - Due to multi-tenancy and its complexity, it is important how data will be isolated.

6. *Data* Security:
    - Data sanitization techniques should be implemented.
    - Auditing and Certifications should be verifiable.
    - Data Encryption, Key Management. Techniques like PKI, PKCS, KEYPROV (CT-KIP, DSKPP) or EKMI should be implemented.
    - Data/Vendor Lock-in - Exit strategies and other options should be stated in a contract.
    - Data ownership - It should be clear who possesses the data and who is responsible for it.
    - Identity and Key Management - Evidence for the access and authentication is necessary.
    - Implementation of incident response strategies.
    - Monitoring of data security.
    - Implementation of network security strategies.

Some of these requirements presented above have also been considered for the analysis of the OASIS architecture which is to follow in the next section.

5. Privacy risks and guidelines for OASIS Architecture

This section provides an overview of the key elements of OASIS architecture with the aim to identify privacy risks and then provide guidelines for the OASIS platform**.** The key objective of this section is therefore to identify the main components of OASIS platform and the data processed/stored in each of these components that could result in privacy risks. These elements are mainly drawn from the deliverables on the OASIS architecture i.e. D1.2 and D2.1 and further input from the pilot sites and partners.

5.1. OASIS Architecture Overview

OASIS architecture encompasses 3 key sub-systems and aims at gathering and providing data to external services. OASIS is composed of the following sub-systems:

1. **the portal**
2. **data core**
3. **kernel with all the features for accessing data (including the social graph)**

It is important to note that the **data core** can be **stored on different locations**; in the architecture; using the notion of containers. Clearly, there is a single instance per location for the data core. Similarly for the **kernel**, there is a single instance that is distributed over several data centres, which can be hosted by different companies (it is proposed in the pilot, that two data centres will be used). Finally, for the case of the **portal**, there is one instance that will be utilised for the pilot (distributed in two data centres), which can possibly be used across different portals.

The data processed and handled by OASIS are as follows:

- **Personal data populated by end users:** These data are used by the platform to display the right information on the portal: user notification, available services according to the user location and also to manage access right to services and other data. These data are recorded in the **social graph.**
- **Personal data managed by civil servant:** These data are retrieved from services such as the citizen portal. These data are recorded in the **data core.**
- **Business data used and produced by public bodies:** These data can be shared with others stakeholders or completely open and available to everyone. These data are recorded in the **data core.**

It is to be noted that only the components within each sub-system that raise concerns for privacy risks are investigated in relation to the below three main threats.

1. **Personal information threat** - Personal information about a user being collected, used, stored and/or propagated in a way that would not be in accordance with the wishes of this user.
2. **Access threats** - People getting inappropriate or unauthorized access to personal data in the cloud by taking advantage of certain vulnerabilities, such as lack of access control enforcement, security holes, data being exposed 'in clear', policies being changeable by unauthorized entities, or uncontrolled and/or unprotected copies of data being spread within the cloud.
3. **Legal non-compliance threat**: The threat of Legal non-compliance and in particular, trans-border data flow legislation may apply, and also some of the data may count as sensitive data in a legal sense, depending upon the jurisdiction, and more restrictive legislation about its treatment apply as a result.

The main ISO standards and sources that include the industry best practices have been followed to perform these analyses. Some of the key sources used are ISO/IEC 29100 [2], Guidelines on Security and Privacy in Public Cloud Computing [3], Cloud computing security and privacy guidelines published by The European Network and Information Security Agency (ENISA) [4] and finally taking into the considerations of the EU Data Protection [5] and national legislations of the pilot sites (Section 2, D1.31). The results of this analysis and the guidelines for OASIS platform are reported in the subsequent sections.

5.2. Portal Analysis:

OASIS platform includes a portal which is the web interface for users (citizens, professional users, services administrators, providers) providing access to all features of OASIS. It is a unified access to all federated services, with notifications and status to manage all their on-going actions.

Personal Information Threats:

- There is no personal information threat to report as the user intending to register or access the OASIS portal can do so if they only wish to use the OASIS services and it is completely voluntarily.

Access Threats:

- Despite employing architectures designed for high service reliability and availability, cloud computing services can and do **experience outages and performance slowdowns** [3]. As OASIS relies on many services from other service providers for data storage and processing and in the case of temporary outages, it must be prepared to carry on operations without the use of the services that are unavailable for periods when the cloud experiences a serious outage. OASIS contingency plan should address prolonged and permanent system disruptions and support continuity of operations that effect the restoration of essential functions elsewhere.

Legal Non-compliance Threats:

- One of the most common compliance issues facing an organisation is **data location** [3]. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organisation's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

  If there is an instance where the OASIS portal is intended to be located in France, this will mean that personal data of the users accessing each services provided by the portal will be processed in the country where the platform is hosted (i.e. France). Therefore, there is a potential legislative risk of the architecture violating trans-border data flow legislation. This risk is also applicable to other sub-systems of the OASIS architecture and this will be indicated in the respective systems analysis.

Proposed Measures and Guidelines:

It has been proposed that in the case of the portal deployment, there is one instance that will be utilised for the pilot (distributed in two data centres), which can possibly be used across different portals. This will avoid the risk of violating the pilot site's national legislations for personal data protection.

Functional Requirements:

In the case of temporary or serious outages, the level of availability of OASIS and its capabilities for data backup and disaster recovery need to be addressed in its contingency and continuity planning to ensure the recovery and restoration of disrupted cloud services and operations, using alternate services, equipment, and locations, if required [3]. Cloud storage services may represent a single point of failure for the applications hosted there. In such situations, the services of a second cloud provider could be used to back up data processed by the primary provider to ensure

that during a prolonged disruption or serious disaster at the primary's facilities, the data remains available for immediate resumption of critical operations. In addition, having policy, plans, and standard operating procedures in place avoids creating an undue reliance on employing cloud services without sufficient recourse.

In addition, OAISIS manager (Pôle Numérique in France) needs to ensure that the cloud/hosting provider has a transparent **incident response process** in place and sufficient mechanisms to share information during and after an incident. Ensure that the organisation can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment [3].

Legal Requirements:

In general, it is important for the OASIS platform to adhere to the general EU 95/46/EC directive and different national legislations requirements as stated in section 2 and 3 respectively in D1.31. In the case of OASIS portal, as it can be seen as a service, the **OASIS manager will have to declare the processing of personal data** to the national authority on personal data, CNIL.

Furthermore, **if the portal only processes basic personal information of users** (e.g. name, email and data of birth) and there is no request for sensitive data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life) then **there is no need for additional citizen portals to be created in the pilot sites** other than the one portal proposed to be located in France. This is because the **EU Data Protection Directive 95/46/EC** highlights that the Member States should comply with the Directive, an equivalent protection of personal data within the European Union is ensured**; Member States shall neither restrict nor prohibit the free flow of personal data between Member States**.

In the case of transferring personal data to a third country (i.e. Turkey) the Member States should ensure that the third country in question provides an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations.

In addition, the **E-Privacy Directive 2002/58/EC** states that the communications provider needs to secure the confidentiality of processing. 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. Moreover, the provider has the responsibility to inform the subscribers to the service, in case of a particular risk of a breach of the security.

5.3. Datacore Analysis:

The data core is a critical module allowing the storage of data, the access to data (search, read, add, delete, update and qualification) and access to external data. Datacore uses the authentication and rights management modules of the OASIS kernel to control access to data.

This is a key module for privacy concerns as highlighted previously as **personal data managed by civil servant** and **business data used and produced by public bodies** are recorded in the data core using the notion of Data container.

Some data have legal requirements and must be physically hosted in one country: this is taken into account by the concept of container. It is also to be noted that more data will be hosted by a European host in order to be subject to EU law.

The following table presents the identified personal data stored and processed for each of the federated services in the data container database in the OASIS platform.

Service	Deployed Pilot Sites	Processing of personal data	Personal Data Stored in OASIS Data Container
A filing system for electronic documents (Archiland)	France	-	None
A user-centric web portal of basic services*	France, Bulgaria and Catalonia	√ Personal data and special categories of personal data	- name - surname - title - sex - address into the city - mail address if different - birth date - birth city - coming from city (if available) - ID Card (scan) - proof of location into the city (scan) Special category data: Children data - Born or not - First name - Last name - Gender - Date of birth - Guardians (main account or other adult) More detailed list of data on p.26 in D1.31
A crowd-mapping application for public domain management (Ushahidi)	France, Bulgaria and Catalonia	-	None
A software suit for the internal management of local public authorities	France and Catalonia	√	<u>OpenCourrier</u> - name - surname - title - address - mail scan (optional) <u>openCimetiere</u> - name

			- surname - title - address (must be in the city)
Investment Promotion and Business Retention*	Turkey	√	- Organisation (e-Service replicator) - Name, Surname of the assigned user - e-mail - other e-mail (if any) - Tel - Fax - Web - Address - Country
Data Collection from Public and Local Authorities*	Turkey	√	- Organisation (e-Service replicator) - Name, Surname of the assigned user - e-mail - other e-mail (if any) - Tel - Fax - Web - Address - Country
City Planning	France and Italy	-	None
Mapping of territorial economic activities	Italy and Catalonia	-	None
Platform that provides static and dynamic public data (OpenData)	France	-	None
Alternative Tourism Network – based on Content Management System (Joomla)*	Bulgaria	-	None
Financial Management Software	France	-	None

Table 5: Personal data stored and processed for each of the federated services in the OASIS data container database

Personal Information Threats:

- There is a potential risk of **loss of control** for OASIS as it requires a transfer of responsibility and control to the cloud provider over information as well as system components that were previously under the organisation's direct control [3]. The transition is usually accompanied by the lack of a direct point of contact with the management of operations and influence over decisions made about the computing environment. This situation makes the organisation's involved dependent on the cooperation of the cloud provider to carry out activities that span the

responsibilities of both parties, such as continuous monitoring and incident response. Compliance with data protection laws and regulations is another important area of joint responsibility that requires coordination with and the cooperation of the cloud provider.

- The **data sanitization** practices that a cloud provider implements have obvious implications for OASIS security [3]. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. It applies in various equipment refresh or maintenance situations, such as when a storage device is removed from service or repurposed. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

  Therefore in the case of OASIS platform, depending on the hosting provider, there is a risk of , data from a user being physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other users, which can complicate matters.

Access Threats:

- Cloud computing, being a distributed architecture, implies more data in transit than traditional infrastructures. Therefore, there is a threat of **intercepting data in transit**. This risk is also applicable to all other sub-systems of the OASIS architecture but more applicable to Datacore as there will be cross-border data transfer. For example, data must be transferred in order to synchronise multiple distributed machine images, images distributed across multiple physical machines, between cloud infrastructure and remote web clients, etc. Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be considered as possible threat sources.
- There is a possible risk of **data ownership** for OASIS platform if the data stored in OASIS and its ownership rights over the data are not firmly established in the service contract to enable a basis for trust and privacy of data [3].

Legal Non-compliance Threats:

- There is a need to ensure secure privacy measures are in place when it comes to the processing of personal data that involves the transmission of data over a network (i.e. **cross-border data transfers**). As highlighted in the Portal legal non-compliance threats when information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Proposed Measures and Guidelines:

To allow for different kind of storage implementations, **Oasis Datacore** introduces the concept of standalone Container, to store personal data and data of applications. Each container has its own administrator, its own database software, and can be localized in a specific datacentre in any of the pilot site in the OASIS cloud. OASIS architecture allows the personal data of users to be stored in different location by using the notion of the containers. Thereby, reducing the risk of violating national legislations over personal data storage and processing.

Functional Requirements:

In the case of **data sanitization**, **OASIS manager** needs to make sure the hosting provider's service level agreements (SLA) should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle [3].

Legal Requirements:

In terms of **data ownership**, OASIS manager should make sure that ideally, the contract should state clearly that the organisation retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organisation's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

In terms of **cross-border data transfers**, the **EU Data Protection Directive 95/46/EC** highlights that the Member States should comply with the Directive, an equivalent protection of personal data within the European Union is ensured; **Member States shall neither restrict nor prohibit the free flow of personal data between Member States**. However, in the case of transferring personal data to a third country the Member States should ensure that the third country in question provides an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations.

In addition, the **E-Privacy Directive 2002/58/EC** states that the communications provider needs to secure the confidentiality of processing. 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. Moreover, the provider has the responsibility to inform the subscribers to the service, in case of a particular risk of a breach of the security.

In France, the French national legislation and according to the national authority on personal data, CNIL, services provided by OASIS are not subject to the Data Protection Act. It's the responsibility of the Public Body (PB) who acquires such software to verify the software not to be in breach of the law. In particular, PB should ensure that the software has a function for deleting and/or archiving personal data. In addition, it is useful to consider the input fields of citizen portal to verify that data collected are relevant to the purpose of the treatment.

The Bulgarian Personal Data Protection Act (PDPA) is strict with regard to **cross-border data transfers**. The PDPA expressly stipulates that transfers of personal data to other Member States of the EU are allowed. For all other transfers, the approach of the Directive 95/46/EC is adopted. Transfers are allowed in substantially the same circumstances, but subject to an overall requirement that a permit by the Data Protection Authority is required. Hence the transfer of personal data outside of the EU and the EEA should be permissible only on condition that the recipient state can ensure an adequate level of personal data protection within its territory.

In Italy, the Data Protection Code relating to the protection of personal data (D. Lgs. 196/2003) guarantees **the free exchange of non-sensitive and non-personal data within the EU**. The services in use in the Italian Pilot work with data of public domain such as, names of the economic

activities and destination of use of the territories of municipalities. Since the data are of public domain, an identification of the user is not mandatory.

In Spain, there is a legal framework for the Protection of Personal Data. The framework is comprised mainly by a central Act (REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal). All the public bodies must follow this legal framework in the implementation of the online public services. Additional security and privacy issues are included within the Legal Framework for the implementation of online public services. It is comprised mainly by the Act on Citizen electronic access to Public Services, the Royal Decree for the Implementation of the National Secutrity Framework and the Royal Decree for the Implementation of the National Interoperability Schema. Blau Advisors will follow the above regulations and guidelines and will work closely with Brunel University to ensure full compliance in all areas.

The main elements for ensuring that the service will be developed according to the law are that in the moment of starting the service provision the public body must:

- Obtain the explicit authorisation of the citizen to share personal data with other Public Bodies with the purpose of managing the citizen request made
- Obtain the explicit authorisation of the citizen to retrieve personal data from other Public Bodies with the purpose of validating and verifying the personal situation according to the citizen request made

In Turkey, unlike the other pilot sites which are all member states of the EU, the Turkish legislation **does not define an overarching framework for data protection**. There is no restriction on cross-border transfers. However, there is a need to adhere to the Draft Law on the Protection of Personal Data which is an effort to comply with the EU Data Protection Directive 95/46/EC.

5.4. Kernel Analysis:

The kernel provides the functions of OASIS to portal and external services, and including the catalog of all data sources and all services. It encompasses and provides the following services:

- authentication and notification process
- access rights management
- management of users
- entities and their relationships (social graph)
- a resource catalog
- a logging mechanism with the management of indicators

Social graph and authentication have been identified as the two key components of the kernel posing potential privacy and legal security risks and therefore have been analysed in detailed in the following subsections.

5.4.1. Social Graph Analysis:

As reported in section 3.3 (D1.2), the social graph module contains confidential private data (i.e. relationship between entities) that allows OASIS to manage users, define access rights and create relationship links between users. The general principles of social graph process to perform these actions have been reported in section 3.3 and this section has been used as the basis to analyse and identify any potential threats to privacy resulting in a risk of privacy violation.

The social graph allows for **storing user personal data** and the **relationship between entities (i.e. persons and organisations)**. This module therefore needs to ensure that relevant privacy and security measures are taken into consideration to safeguard the contained confidential data.

Personal Information Threats:

- There is no personal information threat to report as the user intending to register or access the OASIS portal can do so if they only wish to use the OASIS services and it is completely voluntarily.

Access Threats:

- There is a potential threat for the OASIS portal derived from **misuse by people** who are authorized to access the information. Besides the threats posed by unauthorized access, there is also the risk that people who are authorized to access the personal information of user database by using their privileges for malicious purposes. This could be the result of a deliberate organisational strategy; the action of a malicious individual acting on his own; or the action of a well-meaning individual who is tricked through social engineering attacks or coerced to disclose the information (e.g., by the secret services or the police) [6]. One of the problems of insider attacks is that they are very difficult to detect, as all the accesses to the database would have been authorized accesses.

Legal Non-compliance Threats:

- The laws on data privacy as per the data protection directive 95/46/EC **prohibit allowing a single file to contain all data** so therefore there is a threat of privacy violation.
- As the social graph allows the delegations of rights for users such as children (underage user), persons under guardianship, etc., there is also a need to take **extra pre-caution to manage the data related to users such as children**. The delegation of rights in the Social Graph requires the creation of relationship links between users and this raises concerns. For example as highlighted in section 3.3 (D1.2), a person under guardianship does not necessarily want information revealed to any other user. In addition, these links can be confidential towards one of the extremities. For example, a father who has left his family would not necessarily want that his child to find him.

Proposed Measures and Guidelines:

The OASIS platform has taken considerable steps to ensure that the social graph module does not violate personal data. For instance, social graph is only accessible through “Social Graph Requester” and "Rights Management" modules. Additionally, in accordance with the data separation principle to improve privacy of personal data even towards the administrators of the OASIS system, the social graph does not directly contain personal data, but only their identifiers.

Furthermore, , it is to be noted that it is proposed in D1.2 that the Social Graph in OASIS, unlike the classic social networks, does not allow users to make a wide search to identify other users on the OASIS social graph, thus allowing all users to remain private and not searchable on OASIS platform. This eliminates some potential risk of violating any privacy risks.

Additionally as also proposed it is necessary to separate "silos" so some data may not be in the same file set. OASIS platform therefore **needs to strictly ensure that it breaks this “silos”** as reported in D1.2. Social Graph module needs to therefore make sure that it will provide advanced features to avoid federated services having access to personal data that they don't strictly need. Thereby allowing users to be able to control precisely who are able to read their personal data, when, and why.

Functional Requirements:

In the case of above highlighted access threats such as unauthorised access due to hacking (e.g. Distributed Denial of Service – DDOS Attacks), malicious insider leading to misuse of data etc., OASIS manager therefore needs to ensure the following requirements..

In the case of hacking and generally against access threats, it is recommended that OASIS as proposed in D2.1, is to implement a robust authentication system that includes:

- password management and means of identifying the identity (card, biometrics ...)
- management of access sessions
- access security: two factor authentication

Additionally, in the case of malicious insider, while usually less likely, the damage which may be caused by malicious insiders is often far greater. Therefore, cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers [4] .

Apart from requirements generated for access threat, there is also a need to address the legal non-compliance threat as part of the social graph when it allows for the delegations of rights for users such as children (underage user), persons under guardianship, etc. As a result of the legislative implications (see below legal requirements), there is a need for functional requirement where the OASIS manager needs to ensure that information (e.g. personal contact information) regarding the legal representative who provides the information regarding a child or for an adult under guardianship need to be also stored in the Social Graph and in the datacore.

Legal Requirements:

Generally, the Social Graph sub-system is acceptable to be implemented as part of OASIS platform by strictly adhering to the basic principles highlighted in *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [2], by the Organisation for Economic Co-operation and Development (OECD) as reported in section 2.1 in deliverable D1.31.

In the case of handling children's personal data (underage user), as per Article 29 of Directive 95/46/EC guidelines as highlighted in subsection 2.2.4 D1.31, the protection of children's personal data is fundamental. In situations in which the best interest of the child and his/her right to privacy appear to compete, data protection rights may have to yield to the principle of best interest. The principles of child's best interest and strict purpose limitation should be the criteria in the processing of such information. Therefore there is a need for Social Graph component to adhere to the general principles highlighted in section 2.2.4 (D1.31).

Apart from this, with particular attention to the context of Social Graph and delegation of rights, it is important to adhere to the guidelines specified under the section "Representation" in *Article 29 Data Protection Working Party* [7] .

Based on "Representation" section in Article 29, it recommends that "Children require legal representation to exercise most of their rights". However, this does not mean that the legal representative's status has any absolute or unconditional priority over the child's - because the child's best interest can sometimes confer upon them rights relating to data protection which may override the wishes of parents or other legal representatives. Nor does the need for legal representation imply that children should not, from a certain age, be consulted on matters relating to them.

Additionally, if the processing of a child's data began with the consent of their legal representative, the child concerned may, on attaining majority, revoke the consent. But if he wishes the processing to continue, it seems that the data subject need give explicit consent wherever this is required.

Ultimately, it must be remembered that the rights to data protection belong to the child, and not to their legal representatives, who simply exercise them. This also applies to any legal representative who acts on behalf for a child or young person, or for an adult under guardianship.

Apart from “Representation” guidelines, Article 29 [7] also highlights that the data protection needs of children must take into account two important aspects will be applicable to **Social Graph** module.

1. Firstly, the varying levels of maturity which determine when children can start dealing with their own data and;
2. Secondly, the extent to which representatives have the right to represent minors in cases where the disclosure of personal data would prejudice the best interests of the child.

In terms of right to access, it is normally exercised by the legal representative of the child, but always in the interest of the child. Depending on the degree of maturity of the child, it can be exercised in his/her place or together with him/her. In some cases the child may also be entitled to exercise his/her rights alone. Overall, the criteria for the conditions of access will be not only the age of the child, but also whether or not the data concerned were provided by the parents or by the child – which is also an indication of his/her degree of maturity and autonomy.

Furthermore, as reported Social Graph needs to make sure that it will provide advanced features to avoid federated services having access to personal data that they don't strictly need. Thus, fulfilling the privacy principle requirements [8].

Finally, with regards to the security countermeasures to protect the data the guidelines recommend that “**special care and attention should be exercised in relation to children’s data”**. Security measures should be adapted to the children’s conditions. It should be noted that children may be less aware than adults of the risks that can affect them”.

5.4.2. Authentication Analysis

The OASIS platform provides a **centralized authentication mechanism**, allowing the users to authenticate only once. This feature is widely requested in D1.1, by pilot sites and services providers. It’s the first feature of OASIS, the minimum level of integration.

At this stage, it has been proposed in deliverable D1.2 that only one method of authentication is to be implemented to simplify the developments and maintenance. OASIS platform uses OAuth2 which is adopted by most of the established web services.

As part of the authentication module, the identity management element is where a unique identifier is assigned to each user (citizen) in OASIS and identifies him throughout all the components: Broker, Service Provider and Data Provider. A set of **personal data (name, date of birth, email address, postal address)** is also attached to a user ID.

The OASIS authentication architecture diagram can be referred to in detail in D2.1 in section 2.5.3.

Personal Data Protection Threats:

- There is no personal information threat to report as the user intending to register or access the OASIS portal can do so if they only wish to use the OASIS services and it is completely voluntarily.

Access Threats:

- There is a potential risk of loss of encryption keys as a result of disclosure of secret keys (SSL, file encryption, customer private keys, etc) or passwords to malicious parties, the loss or corruption of those keys, or their unauthorised use for authentication and non-repudiation (digital signature).
- It is reported in section 3.1.1 (D1.2) that during the process of change of password by the user, if the normal procedure fails, a temporary account is created without the user's personal data. The user then has to call the OASIS support and prove their identity to be able to reinitialize the user's password and merge the temporary account with the normal account. There is no clear indication of the process involved for the identity verification over the phone which causes concern for potential privacy violation.

Legal Non-compliance Threats:

- As the OASIS platform is based on a single security/authentication module, this will mean that personal data of the users accessing each services provided by OASIS will be stored in the country where the platform is hosted (i.e. France). For instance, as each person is associated with a globally unique identifier in OASIS, which identifies his personal data. Identity data (name, mailing address, email, phone number, etc.) is stored in the social graph, keyed by the unique identifier.

Proposed Measures and Guidelines:

The OASIS platform has taken substantial steps to ensure a **good level of authentication system** and this is detailed in D2.1. For example, If the user creates a password to log into OASIS, he/she's given the option to enable strong authentication (at any time and reversibly), in the form of two-factors authentication (using a one-time password in addition to the password associated with the account). The one-time password has either been generated earlier (list of scratch codes) and printed by the user or generated by a third-party application based on the current time and with an expiration window (*Time-based One-Time Password*, TOTP, standardized by RFC 6238.).

In the case where user forgets their password, the user can request it to be reset. An email is then sent with a one-time link to reset the password and enter a new one (if strong authentication is enabled for the account, the second factor must be used too.) Any change in the means of authentication automatically triggers an email. Similarly, in case the email address for the account is changed, a message is sent to the previous email address. Any change requires the use of the second factor (if strong authentication has been enabled for the account).

Furthermore, OASIS takes good control over the level of strength of passwords by avoiding implementing to authenticate with a third party account (e.g. Google, Facebook, etc). This also better insures the privacy settings of personal data.

Apart from the authentication system, OASIS also has proposed robust security measures (see section 2.5.2 in D2.1 for more detail) that also need to be implemented. For instance:

- All communications need to occur over a secure connection (TLS)

- In case a Service Provider or Data Provider is compromised, its password can be changed (preventing new authorization requests or validation of tokens), and all the tokens associated with this provider can be revoked (preventing validation of tokens by other Data Providers). This is all centralized at the authentication module, the only warrant of the validity of those credentials. The Service Provider may revoke a token automatically if it considers that it has been compromised (e.g. very high number of requests in a short timeframe and possibly on several Data Providers); similarly, a provider can be temporarily locked-out, automatically, if the profiling of its requests seems abnormal (e.g. abnormally high number of requests in a short timeframe and possibly on several Data Providers, but using different access tokens). The Data Providers may wish to use similar mechanisms by themselves to further secure their data.
- The authentication module should not store any sensitive information other than (hashed) user passwords (if any) and the various codes and tokens required by the security protocols.

These measures need to be strictly ensured that they are implemented as part of platform by the OASIS manager.

Functional Requirements:

In terms of Kernel, OASIS manager needs to ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organisation.

According to Electronic Authentication guideline published by National Institute of Standards and Technology (NIST), there are four levels of authentication based on the level of security needed [9]. The guideline in the document states the necessary requirements levied upon the authentication process to achieve the required threat resistance at each assurance level. Therefore the OASIS platform needs to **maintain at least at Levels 2 and above where the authentication** process shall provide sufficient information to the Verifier to uniquely identify the appropriate registration information that was (i) provided by the Subscriber at the time of registration, and (ii) verified by the RA in the issuance of the token and credential. However, it is important to note that these requirements will not protect the authentication process if malicious code is introduced on the Claimant's machine or at the Verifier.

Legal Requirements:

It is important to take into consideration the general principles of EU 95/46/EC directive and different national legislations requirements as stated in section 2 and 3 respectively in D1.31. There are no other special legal requirements.

5.5. Conclusions

This section focused on identifying privacy risks and providing guidelines for the OASIS architecture based on its use of cloud computing technologies. There was a need to ensure privacy risks were identified and addressed as the OASIS architecture has key sub-systems which processes/stores data. This was achieved by identifying three main threats (i.e. Personal information, Access and Legal non-compliance threats) and then highlighted the proposed measures taken by the OASIS platform to ensure privacy risks and also providing additional functional and legal requirements to each of the sub-system of the OASIS architecture. The following table presents the summary of the key privacy and functional requirements for the OASIS architecture.

OASIS Architecture Components		Privacy and Functional Requirements for the OASIS architecture	
		Functional Requirements	**Legal requirements**
Portal		• In the case of temporary or serious outages, OASIS manager has to ensure the level of availability of OASIS and its capabilities for data backup and recovery need to be addressed in its contingency and continuity planning to ensure the recovery. • OAISIS manager needs to ensure that the cloud/hosting provider has a transparent incident response process in place and sufficient mechanisms to share information during and after an incident. This should then be conveyed to the users of the OASIS portal.	• As OASIS portal can be seen as a service, the OASIS manager will have to declare the processing of personal data to the national authority on personal data, CNIL. • If the portal processes basic personal information such as name, email, date of birth of users and there is no request for sensitive data such as social security number there is no need for additional citizen portals to be created in the pilot sites other than the one portal proposed to be located in France only. • In the case of security breach, according to the E-Privacy Directive 2002/58/EC, the provider has the responsibility to inform the subscribers of the service.
Data Core		• OASIS manager needs to make sure the hosting provider's service level agreements (SLA) should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle	• OASIS manager should make sure that ideally, the contract should state clearly that OASIS retains exclusive ownership over all its data; that the cloud/hosting provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use OASIS's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. • In terms of cross-border data transfers, the EU Data Protection Directive 95/46/EC highlights that the Member States should comply with the Directive, an equivalent protection of personal data within the European Union is ensured; Member States shall neither restrict nor prohibit the free flow of personal data between Member States.
Kernel	**Social Graph**	• To implement a robust authentication system that includes: o password management and means of identifying the identity (card, biometrics ...) o management of access sessions o access security: two factor authentication • OASIS manager needs to ensure that information (e.g. personal contact information) regarding the legal representative who provides the information regarding a child or for an adult under guardianship need to be also stored in OASIS Social Graph and the datacore.	• Social Graph sub-system is acceptable to be implemented as part of OASIS platform by strictly adhering to the basic principles highlighted in Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as reported in section 2.1 in deliverable D1.31. • It must be noted that in the case of access rights and specifically children data, it must be remembered that the rights to data protection belong to the child, and not to their legal representatives, who simply exercise them.
	Authentication	• OASIS platform needs to maintain at least at Levels 2 and above where the authentication process shall provide sufficient information to the Verifier to uniquely identify the appropriate registration information that was (i) provided by the Subscriber at the time of registration, and (ii) verified by the RA in the issuance of the token and credential.	• It is important to take into consideration the general principles of EU 95/46/EC directive and different national legislations requirements as stated in section 2 and 3 respectively in D1.31.

Table 6: Summary of the privacy and functional requirements for the OASIS architecture

6. Changes to the services provided by OASIS

This section reports the changes to the several services that will be available through the different pilot and some of which are shared among the different sites. Table 8 depicts the updated correlation among sites and services since the submission of D1.31. The succeeding sub-sections will report the changes to detailed description of the data flow for each of the services, with the aim to identify any additional potential threats to privacy resulting in a risk of privacy violation.

		Pilot sites				
		Pôle Numérique	David Holding	EMDA	Turin Province	Blau Advisors
Services to be offered in Pilot B demonstration	A filing system for electronic documents (Archiland)	●				
	A user-centric citizen web portal of basic services*	●	●			●
	A crowd-mapping application for public domain management* (Ushahidi)	●	●			
	A software suit for the internal management of local public authorities* (6 services)	●				●
	Investment Promotion and Business Retention*			●		
	Data Collection from Public and Local Authorities*			●		
	City Planning	●			●	
	Mapping of territorial economic activities*				●	●
	Platform that provides static and dynamic public data (OpenData)	●				
	Alternative Tourism Network – based on Content Management System (Joomla)*		●			
	Financial Management Software*	●				

Table 7: List of deployed services offered by each site

Key Notes and Changes:

- * Denotes that the particular service has been revised since the submission of D1.31.
- Services that are no longer provided since the submission D1.31 and therefore not included in Table 7:
  - Monitoring the progress in projects funded by a development agency
  - Cluster development and management
  - E-Gov Platform (Ready)
- Catalonia has been introduced as a new pilot site with the exit of Comune di Bussoleno.

- Financial management software is a newly introduced service as Pole Numerique will no longer use the Investment Promotion and Business Retention provided by EDMA. More information on this service is reported in the subsequent sub-sections.

The subsequent sections present a detailed explanation of the changes only on the services that have had a change which have been indicated by an asterisk in Table 8.

6.1. A user-centric web portal of basic services

The user centric web portal of basic services is no longer referred to as Capdemat. This service offering basic public services is now shared by France, Bulgarian and Spanish pilot sites offering their own respective services and is yet to be developed. It is important to note that Commune di Bussoleno pilot site will no longer use this application to provide any service to citizen on the OASIS platform.

In France, the Drome pilot site will provide the same public services such as school registration, canteen payment, etc. as stated in D1.31. As a result, there are no changes to service provided by the Drome pilot site.

In the Bulgarian pilot site there is additional information reported on the service description and use case since the submission of D1.31 which is reported below.

The pilot site aims to provide web portal basic services using OASIS portal as front end and Archimed eDMS (electronic document and workflow management system), that is used at large number of public authorities, as the internal software for managing the citizen requests. This application and set of services are included to replace Capdemat application and to demonstrate that OASIS concept allows integration of existing services at least at portal level. Archimed Online Services is a front end decision of Archimed eDMS, providing an opportunity for the provision of electronic services over the Internet for external users-citizens, companies, governmental and municipal organisations, etc. The module is especially useful for companies from the sectors of utilities and organisations in the sphere of State and municipal administration, who actively communicate with citizens, businesses and other subscribers to the service. The aim of the module is to provide handy tools for remote electronic services to external users for an organisation, save time and effort, as well as to reduce the load on the staff working in the front offices of the organisation. The module enables external users to sign documents (applications, applications, service requests, complaints, etc.) through the Internet, and thus initiate the automatic startup of the internal process for handling their request in the Archimed eDMS.

This module will be replaced by the OASIS portal and will allow:

- Service request initiation by a citizen or a company electronically;
- Check the status of your requested service from a citizen or company electronically.
- Receipt of the result of the execution of the service electronically when initiating service, external users (citizen or company) selects the service from the list shown in the website of the organisation fills in the fields in the on-screen form and confirm your registration. As a result, the system automatically starts the process of implementing the requested service, eProcess Archimed and returned to the applicant for information concerning the registration and the date of the index registered document, as well as the link for access to check the status of processing. The same information is sent to the e-mail address indicated by the applicant. The service is handled by the authorized officers of the organisation by Archimed eProcess Toolbox, such as the system automatically delivers all the necessary information to contractors, according to the technological processing of card service, and monitor the deadlines of each

stage. At any time after the initiation of the service electronically, the applicant can check its current status of processing using sent to him at the time of initiating the link for access.

The following Use Case describes the main functionalities of the service provided by Bulgarian pilot site:

Use Case:	Various services for citizen and business
Goal in Context:	
Primary Actors:	Citizen, Business
Secondary Actors:	Government agencies, Municipalities
Stakeholders & Interests:	**Citizen and Business:** They can register requests at any time, by means of a convenient WEB forms. Monitor the movement of their inquiries and to receive answers electronically. **Government agencies and Municipalities:** Can become more flexibility in the management of citizens and business request.
Trigger:	1. **"**Push" mode – The applicant chooses the appropriate form from a list and fills fields. The system checks the validity of the entered information. The application shall be signed electronically by the applicant. The system checks the validity of the digital certificate. In case of valid certificate, the request will be registered in the back office. The applicant returns a unique entry number.
Preconditions:	The applicant must has valid digital certificate from trusted "Certificate service provider"
Success End Condition:	
Failed End Condition:	
Data processed and managed:	1. Applicant accesses WEB site with services 2. Applicant selects appropriate service. 3. Applicant fills data – Input: Data (depends of service), Output: OK from the system if data is valid, "Correct errors" if data missing or not valid. 4. Applicant sign form by his own digital certificate – Input: Digital certificate, Output: OK if certificate is valid, "Refuse" – certificate is not valid 5. If all checks are OK system will register the request and will return unique ID to the applicant, else will return reject.

It is important to note that the data that are processed by the Back Office system fall under the data protection act of Bulgaria. Therefore, **all the data are property of the State/Municipality and may not be publicly available**. Front end system can only submit requests (digital signed) and receive responses for that particular user (digital signed).

Additionally, this service is also going to be deployed in Catalonia. More information on the use cases and data sets will be provided in January.

In Catalonia, the usage of this service is intended to allow the citizens to interact with the public bodies using a set of forms that will cover two-way communication. This is new for the public bodies involved in the pilot site as the existing tools available for this small municipalities only

cover web based communication from citizen to public body being the returning path via email or post mail. The created forms will cover the collection of information for triggering the new applications created for the OpenMairie project.

The service will be delivered according the following use cases:

- Submission of environmental services incidences communicated to the public body.
- Management of request for grant and subsidy concession.

Use Case:	Communication of environmental incidences
Goal in Context:	Improve the communication from citizen to public bodies for solving faster and under a more efficient manner the incidences appearing while public bodies deliver environmental related services.
Primary Actors:	Citizen, Business
Secondary Actors:	County councils, Municipalities and subcontractors
Stakeholders & Interests:	**Citizen and Business:** They can register requests at any time, by means of a convenient WEB forms. Monitor the movement of their inquiries and to receive answers electronically. **Government agencies and Municipalities:** Can become more flexibility in the management of citizens and business request.
Trigger:	1. **"**Push" mode – The applicant chooses the appropriate form from a list and fills fields. The system checks the validity of the entered information. The request will be registered in the back office.
Preconditions:	
Success End Condition:	
Failed End Condition:	
Data processed and managed:	1. Applicant accesses WEB site with services 2. Applicant selects appropriate service. 3. Applicant fills data – Input: Data (depends of service), Output: OK from the system if data is valid, "Correct errors" if data missing or not valid. 4. If all checks are OK system will register the request.

Use Case:	Subsidy management
Goal in Context:	Allowing the citizen to apply for grants and subsidies using an online channel.
Primary Actors:	Citizen,
Secondary Actors:	County councils, Municipalities
Stakeholders & Interests:	**Citizens:** They can register requests at any time during the call is open, by means of a convenient WEB forms. Monitor the movement of their inquiries and to receive answers electronically. **Government agencies and Municipalities:** Can become more flexibility in the management of citizens and business request.
Trigger:	1. **"**Push" mode – The applicant chooses the appropriate form from a list and fills fields. The system checks the validity of the entered

	information. The request will be registered in the back office.	
Preconditions:	The call must be open by the public body. The citizen must have a valid digital certificate	
Success End Condition:	All the data is correct and the digital certificate could be used for the signature	
Failed End Condition:	Data or digital certificate are not valid	
Main Success Scenario:	1. User access to the platform	Input : user/password) Output : None
	2. User select the form for the grant and fill it in	Input: Data in the form Output: validation
	3. User is prompted to electronically sign the form.	Input: Citizen's action including the acceptance of the transmission of personal data and allowing the public body to retrieve on behalf of him/her personal information to other public bodies Output: -Request for digital certificate validity -display success of signature -submission of personal data
	4. the user can monitor the evolution of the request	
	5. Provide additional information if the public body request it.	Input: Data in the form or documents Output: validation:
Data processed and managed:	1. Data for the request 2. Attached documents 3. Additional data provided 4. Resolution of the request provided by the public body	

6.2. A crowd-mapping application for public domain management (Ushahidi)

Ushahidi service is now shared by France and Bulgarian pilot sites offering their own respective services. It is important to note that Commune di Bussoleno pilot site will no longer use this application to provide any service to citizen on the OASIS platform.

The pilot sites in in France and Bulgaria will provide the same public services as stated in D1.31. As a result, there are no changes to service provided by these two pilot sites.

6.3. A software suit for the internal management of local public authorities (OpenMairie)

There haven't been any technical changes for this service since the submission of D1.31 but it is now shared used by French and Spanish pilot sites.

The usage of the service in the Spanish pilot site implies the creation of new back office processes for the treatment of currently not covered internal processes as well as the reuse of the existing ones. For the reuse of the existing ones there is no changes on the provided use cases for the French pilot.

The new use cases appearing are:

- Submission of environmental services incidences communicated to the public body.
- Management of request for grant and subsidy concession.
- Public purchase management

In all the cases the service development includes the treatment of public and private data. The interaction with the user will be limited to the civil servants involved in the process for the two first cases and for the tenderers and the civil servants in the third use case.

Use Case:	Management of environmental incidences
Goal in Context:	Improve the communication from citizen to public bodies for solving faster and under a more efficient manner the incidences appearing while public bodies deliver environmental related services.
Primary Actors:	County councils, Municipalities and subcontractors
Secondary Actors:	Citizen, Business
Stakeholders & Interests:	**Government agencies and Municipalities:** Can become more flexibility in the management of citizens and business request. **Citizen and Business:** They can register requests at any time, by means of a convenient WEB forms. Monitor the movement of their inquiries and to receive answers electronically.
Trigger:	1. **"**Pull" mode – when the applicant submits the request a new process is triggered and automatically assigned to a civil servant.
Preconditions:	
Success End Condition:	
Failed End Condition:	
Data processed and managed:	1. The request is received by the civil servant 2. A corrective action is applied 3. If the problem persists a new solution or a new application of the original is applied. 4. If solved, a communication to the requester is made

Use Case:	Subsidy management
Goal in Context:	Allowing the citizen to apply for grants and subsidies using an online

	channel.	
Primary Actors:	County councils, Municipalities	
Secondary Actors:	Citizen,	
Stakeholders & Interests:	**Government agencies and Municipalities:** Can become more flexibility in the management of citizens and business request. **Citizens:** They can register requests at any time during the call is open, by means of a convenient WEB forms. Monitor the movement of their inquiries and to receive answers electronically.	
Trigger:	1. **"**Pull" mode – when the applicant submits the request a new process is triggered and automatically assigned to a civil servant.	
Preconditions:	The civil servant must have a valid digital certificate	
Success End Condition:	The digital certificate could be used for the signature	
Failed End Condition:	Digital certificate are not valid	
Main Success Scenario:	1. Civil servant access to the platform	Input : user/password) Output : None
	2. Civil servant selects the request and work on it and make a decision for its approval, rejection or request for more data	Input: Data in the form Output: validation
	3. If approved or rejected the civil servant signs the resolution and deliver it to the citizen portal.	Input: Citizen's action including the acceptance of the transmission of personal data and allowing the public body to retrieve on behalf of him/her personal information to other public bodies Output: -Request for digital certificate validity -display success of signature -submission of personal data
	4. If more data is needed, the civil servant ask for it through the citizen portal and waits	Input: Sliding action Output:
	5. Provide additional information.	Input: Data in the form or documents Output: validation
Data processed and managed:	1. Data for the request 2. Attached documents 3. Additional data provided 4. Resolution of the request provided by the public body	

Use Case:	Public purchase management	
Goal in Context:	Allowing the management of public tenders using an online channel.	
Primary Actors:	County councils, Municipalities	
Secondary Actors:	Tenderers	
Stakeholders & Interests:	**County councils agencies and Municipalities:** Can become more flexibility in the management of purchasing process. **Tenderers:** They can reduce costs and time in the process of participation in public tenders.	
Trigger:	1. **"**Pull" mode – when the public body opens a call a new process is deployed.	
Preconditions:	The civil servant and the tenderers must have a valid digital certificate	
Success End Condition:	The digital certificate could be used for the signature	
Failed End Condition:	Digital certificate are not valid	
Main Success Scenario:	1. Civil servant access to the platform	Input : user/password) Output : None
	2. Civil servant initiates the process by defining the needed data	Input: Data in the forms Output: validation
	3. Tenderers present the bids	Input: Tenderers access to the forms and provide data and documents. Signature of the form and its content. Output: -Request for digital certificate validity -display success of signature -submission of data
	4. civil servants select the most suitable bid	Input: Civil servant access to the forms and selects the winner. Signature of the form and its content. Output: -Request for digital certificate validity -display success of signature -submission of data
	5. Communication to the tenderers and contracting.	Input: Data in the form or documents Output:
Data processed and	1. Data for the request	

managed:	2. Attached documents 3. Additional data provided 4. Resolution of the request provided by the public body

6.4. Investment promotion and business retention

This service was initially planned to be deployed in Turkey and France. However it is no longer deployed in the French pilot site due to significant difference in legislation between the French and the Turkish pilot sites.

There are no reported technical changes for this service in the case of Turkish pilot site since the submission of D1.31 but there is additional information on the use cases of this service from EDMA which are reported below. The detailed service description and the use cases of this service can be referred to in **deliverable D1.31 and D1.1.**

It has been reported that there are two groups of users for this e-service:

- **First group of users**: Service replicators who will deliver the e-service in their territory
- **Second group of users**: Service end-users, i.e. public officials who will use the e-services delivered by the service replicators.

The following table presents the detailed description of the data that are processed and stored for some of the use cases of the service. It is to be noted that the same data sets that are processed for different use cases are not repeated below.

Relevant requests performed by the **first group of users** and the relevant data:

Request	**Data**
User-Service Replicator account verification (Investment Promotion and Business Retention)	- Organisation (e-Service replicator) - Name, Surname of the assigned user - e-mail - other e-mail (if any) - Tel - Fax - Web - Address - Country
User-Service Replicator End-User/Company representative account and profile management section Edit user profile associated with an account	<u>User details</u> - Name - Surname - Company - Company's field of specialisation - Last year's Total Annual Sales/Operations - Total number of employees - Function in the Company - Year of incorporation

	- e-mail - other e-mail (if any) - Tel - Fax - Web - Country - Address
User-Service Replicator User Request Editing section (Investment Promotion and Business Retention)	<u>Edit submitted Investor form</u> Same user details as above but in addition: Planned Investment and Requested Assistance - Sector to invest - Requested investment assistance - Target market or sector - Estimated size of fixed investment - Investment timeframe (Estimated start and end dates) - Estimated employment to be created - Vocational training required for personnel - Partnership if any (already existing or prospective) - Basic requirements - Type and amount of waste to be created - Preferred areas <u>Edit Meeting Request form</u> Same user details as above but in addition: Details of Request for the Meeting - Purpose of the Meeting - Number of the meeting participants from your side - Highest ranking executive or officer from your side to be participating - "Preferred meeting place - (for directions for our offices please check About us section) - Any further information you would like to share <u>Edit Complaint/Suggestion form</u> Same user details as above but in addition: Details of Complaint • Name of natural or legal person(s) that the complaint is placed against • Details of problems encountered • Loss or damage incurred as a result of complained action

	• Requested assistance to correct results of the complained action • Any prior notice about the complaint that has been submitted to any public authority or other natural persons or legal entities Details of Suggestion • Name of natural or legal person(s) that the suggestion is about • Reason(s) for the suggestion • Details of the suggested action(s) Any prior notice about the suggestion that has been submitted to any public authority or other natural persons or legal entities

The following table presents the relevant description of the data that are processed and stored for some of the request performed by the **second group of users.**

Request	**Data**
User-Service Replicator User Business Angel Networking editing section (Investment Promotion and Business Retention):	<u>Edit submitted Entrepreneur form:</u> <u>User details</u> - Name - Surname - Company - Company's field of specialisation - Last year's Total Annual Sales/Operations - Total number of employees - Function in the Company - Year of incorporation - e-mail - other e-mail (if any) - Tel - Fax - Web - Country - Address Planned Investment and Requested Assistance - Sector to invest - Target market or sector - Estimated size of fixed investment - Investment timeframe (Estimated start and end dates) - Estimated employment to be created - Partnership (already existing or prospective) - Type and amount of waste to be created

	Preferences for Angel Investor being sought - Type of Angel Investor sought - Amount of equity finance needed - Type of financing needed - Distribution of shares and management rights offered

6.5. Data collection from Public and Local Authorities

There haven't been any technical changes for this service since the submission of D1.31 but there is additional information on the use cases of this service which are reported below. The service description and the use cases of this service can be referred to **deliverable D1.31 and D1.1.**

It has been reported that there are two groups of users for this e-service:

- **First group of users**: Service replicators who will deliver the e-service in their territory
- **Second group of users**: Service end-users, i.e. public officials who will use the e-services delivered by the service replicators.

In addition, there is more information on the data processed by this service. The following table presents the detailed description of the data that are processed and stored for the relevant request performed by the **first group of users.**

Request	**Data**
User-Service Replicator account verification	- Organisation (e-Service replicator) - Name, Surname of the assigned user - e-mail - other e-mail (if any) - Tel - Fax - Web - Address - Country
Online invitation to let End-user create account and authorize to feed data	- e-mail address - Province/City/Locality - Organisation - Respective column of the Data form - Assign view/edit authorization
Send messages to the users	- Subject line - Text - Attached document

The following table presents the detailed description of the data that are processed and stored for the relevant request performed by the **second group of users.**

Request	**Data**
Accept online invitation and enter	- Name - Surname

user details	- Organisation - Function - e-mail - other e-mail (if any) - Phone - Fax - Web - Address

6.6. Mapping of territorial economic activities

There haven't been any technical changes for this service reported by the Italian pilot site since the submission of D1.31 but it is now also shared by Spanish pilot sites. This service will therefore be deployed in Italy and Catalonia.

In Catalonia, the areas covered by the pilot site have two main issues in the area of local economical development. On one side there is a lack of knowledge on the availability of certain types of business in the areas making the people to buy far from their living place; On the other hand, people searching for investment opportunities in the area looks for possible suppliers, and there is no tool in order to support both needs. For this pilot site the service provision will represent a reuse of the one in Provincia de Torino by adding the local data and it not implies changes on the use cases.

6.7. Alternative Tourism Network – based on Content Management System (Joomla)

There is now additional information on the use cases of alternative tourism network service deployed in Bulgaria which are reported below. The detailed use cases of this service can be referred to in **deliverable D1.1.**

Alternative Tourism Network service is only to be deployed in Bulgaria and is intended to record events, sites, destinations, suppliers of alternative and any other tourism services. Under alternative tourism services can be considered unorthodox and unorganized all tourist events such as biking, walking hiking with their routes, schedule instructions and landmarks along the route, rest areas, and not least the company or organisation that provides a logistics such an event. This include alternative tourism and rural tourism, cultural history, religion, exoteric and other forms of thematic tourism specific sports such as rafting, Paintball, Airsoft and more. The service can be used by companies organizing this type of events, NGOs organizing themed events. The service will work based on Joomla. The aim of the service is to get a better interaction between tourist organisations and local community. The service will be run and managed by David Holding Company.

The following use case table describes the main functionalities of the service.

Use Case:	Service to record events, sites, destinations, suppliers of alternative and any other tourist services.
Goal in Context:	Organize in one place tourism events from various sources
Primary Actors:	End users of this service are citizens
Secondary Actors:	Travel agencies
Stakeholders & Interests:	**Regional administrations** - Publishing initiatives related to national holidays, holidays from the national calendar as a celebration of Historical Figures and anniversaries. Local (regional) initiatives related to business events such as exhibitions and fairs. **Municipalities** - Publish events related to holidays of the municipality, local Initiatives related to culture, history and lifestyle of the region. Special events related to geography peculiarities of the region allowing the practice of specific types of sport and tourism, rafting, delta planning and more. **NGOs associated with the Arts and Culture** - Publishing initiatives related to cultural events of national or regional importance, such as "Night of Museums", "Days of Opera and Ballet" and others. **Museums, galleries, theatres, opera houses** - Publish information about their performances, exhibitions and other initiatives **NGOs associated with business initiatives and business development at the national and regional level**: These are the "Chamber of Commerce", Agencies for Regional Economic Development, Business associations. They post information about meetings, conferences and other business-related events. **These five types of organisations can be regarded as source of events**. **Hotels, restaurants, complexes for recreation and treatment -** Publish information about services and attractions they offer. **Freelance** - translators, guides, mountain guides, rescuers and others. **These two types of organisations can be regarded as source of resources.** **Travel agencies** - Organize events published by such organisations in packages that offer their customers. Use resources such as hotels, museums, attractions by directly communicating with them to form the final service to the customer. **Customers / Citizen** - Consumers and citizens can easily organize individual packets of events other than those offered by travel agencies. They can also reserve resources such as hotels, restaurants, museum, galleries and etc.
Trigger:	**Data input** **Events -** Events organized by government organisations, ministries, regional administrations, NGOs, businesses, non-profit organisations are introduced in the form of an **annual calendar of events**. Calendars are personalized for each organisation. Occurrences that are entered may be single or, for a period of time.Events over a period of time are composite and follow the hierarchy of main event and sub-events. Personal

	calendars can be connected to another at the level of event. For example, a calendar of regional administration can has event that takes place in the calendar of municipality or other organisation. **Resources -** As resources we can consider all individual physical objects such as hotels, restaurants, special places, museums, galleries, and more. Information is entered by the people serving these sites and this information is mostly static - address, geographic location and etc. Resources can be linked with the events.For example, event "Night of Museums" and resources list of museums. Resources can be represented as a mini Web sites in CMS or external links to the original sites. Each resource can be connected to any number of events and vice versa. All data is entered in the so-called Back office system **Data output –** Calendar(s) with linked resources. The end product of tourist agencies packages aimed at targeting users according to event events. For the ordinary person it is a calendar with resources according to the desires and needs of the user.
Preconditions:	-
Success End Condition:	-
Failed End Condition:	-
Data processed and managed:	1. Registration: Every actor in the system must be registered. During registration introduces the type of organisation and whether it is a source of events or resource. After that the system sets to the organisation name and password, personal calendar or mini Web site. 2. Data entry: Each organisation establish their own calendar with events. Organisations can link events. This can be done according to the type of the event or events taking place. Organisations that are sources of resources, register their services and can link them to one or more events. 3. Travel Agencies: Create their own calendar event / events calendar periods. Calendars of these agencies include links to the original event calendars. Agencies can combine events with other events from different calendars and resources in the service packages that want to offer. 4. Ordinary users, citizen - Registered users can produce their own individual calendars according to their wishes and needs by communicating directly with the sources of events and resources.

The following table presents the detailed description of the data that are processed and stored for the relevant task.

Process	**Data**
User registration	- Name of user - Type of user – type of organisation - Type of source - source of events, resources or both - Address, Region - Phones - E-mails

	- Web addresses - Other contact information - Contact person - name - Contact person – phone - Contact person – e-mail - Contact person – other information
Events registration	- Calendar identity - unique number - Event identity - unique number - Source organisation – which is this calendar - Name of event – Full name of event - Type of event – Here can be various types of events – sport, art, culture and etc. - Start date and time - End date and time - Recurrence - Place – exact place, address, region …etc. - Geography coordinates - Pointer(s) to the sub events - Pointer(s) to the resources – can point to internal web site or to the external one. - Pointer(s) to additional stored information – pictures, text, graphics and etc. – depends on context off information.

6.8. Financial Management Software

The financial management software has been introduced due to a large difference in legislation between the French one and the Turkish one, the service "Investment Promotion and Business Retention" won't be used, but a new service will be tested (a financial management system) as it is the key software for interoperability in Public Bodies. This service will only be deployed in France.

The financial Management inside Public Bodies is at the centre of information flows. It manages the financial transactions related to the management of the public domain, to the purchasing of equipment and materials.

The following use case table describes the use of shared information on companies within the service.

Use Case:	Entering an invoice
Goal in Context:	Management of all the financial issues of a public body
Primary Actors:	End users of this service are civil servants
Secondary Actors:	None
Stakeholders & Interests:	All contractor companies, service providers of public bodies
Trigger:	Entering an invoice
Preconditions:	-
Success End Condition:	-

Failed End Condition:	-
Data processed and managed:	1. The civil servant creates a new invoice to be paid. 2. The civil servant has to link this invoice to the company. Companies list and information are stored in a unique file called "Third party file". 3. After having linked the invoice to the right company, the civil servant can complete the financial statement with additional information: Invoice number, type of service or work, date, amount, internal department beneficiary ....

The following table presents the detailed description of the data that are processed and stored for the relevant task.

Process	**Data**
Companies information shared in the Third Party File	- Name of the company - Company national code (SIRET) - Legal form - Type of activity (NAF national codes) - Address - Phones - E-mails - Name of the Legal Authorized Representative - Position of the Legal Authorized Representative - IBAN account

6.9. Summary of the changes to the services

A summary of the **main changes to the particular services** that have been revised since the submission of D1.31 are presented below.

- **A user-centric web portal of basic services** – This service is no longer referred to as Capdemat. The French pilot site has no reported changes. There is now more additional information on the use case to the service offered by the Bulgarian pilot site, David Holding and for the incorporation of the pilot site in Catalonia.
- **Ushahidi** - There is no technical changes to the service offered by Ushahidi, however Commune di Bussoleno pilot site will no longer use this application to provide any service to citizen.
- **A software suit for the internal management of local public authorities** – No reported technical revisions for the French pilot site. This service is now also deployed in the Spanish pilot site and the information has been incorporated.
- **Investment Promotion and Business Retention** – No reported technical revisions to the service offered by EDMA. There is now more detailed information on the use cases of the service which had been reported.
- **Data Collection from Public and Local Authorities** – No reported technical revisions to the service offered by EDMA. There is now more detailed information on the use cases of the service which had been reported.
- **Mapping of territorial economic activities** - No reported technical revisions for the Italian pilot site. This service is now also deployed in the Spanish pilot site but no other reported changes.
- **Alternative Tourism Network – based on Content Management System (Joomla)** – There is now more detailed information on the use cases of the service offered by David Holding which had been reported.

The introduction of a new service to OASIS deployed in French Pilot Site:

- **Financial Management Software**

The services that are **no longer provided** by OASIS since the submission of D1.31 are presented below:

- **Monitoring the progress in projects funded by a development agency**
- **Cluster development and management**
- **E-Gov services (Ready)**

7. Privacy risks and guidelines for OASIS Services

This section presents any additional privacy guidelines for the OASIS services at each pilot site apart from the guidelines presented in D1.31.

7.1. Privacy guidelines for OASIS Services at Pilot Site 1: France

Within the scope of the OASIS project **Pole Numerique based in France** will test and implement services related to **7 types of applications**:

- Archiland
- A user-centric citizen web portal of basic services
- Ushahidi
- A software suit for the internal management of local public authorities
- City Planning
- OpenData
- Financial Management Software.

In France, the French national legislation and according to the national authority on personal data, CNIL, services provided by OASIS are not subject to the Data Protection Act. It is the use of software for processing personal data that must comply with the requirement of the law. Software vendors have no legal obligation to offer products configured for this purpose. It's the responsibility of the Public Body (PB) who acquires such software to verify the software not to be in breach of the law. In particular, PB should ensure that the software has a function for deleting and/or archiving personal data. In addition, it is useful to consider the input fields of citizen portal to verify that data collected are relevant to the purpose of the treatment.

In other words, the entities that have to make a declaration for processing personal data are:

- The OASIS manager, responsible of processing personal data (social graph) for the use of the platform.
- All PB using a service that process personal data (data core). (OASIS manager is not responsible for the use of personal data by PB).

The procedures that the PB or entities processing personal data must declare to the CNIL for the storage of such information and the purpose of their treatment are as follows:

There are 3 cases that exists:

- Standard declaration for treatment of personal data.
- Simplified or even exemption of declarations for essentials activities such as General Accounting, Management of Human Resources and payment of public sector staff, Management of the electoral register.
- Processing of sensitive data requiring prior authorization under a motivated purpose.

In France sensitive data are as follows:

- Racial or ethnic origin, philosophical, political, trade union, religious opinions, sexual life and health. Treatment can be justified by the public interest where the data are anonymised at short notice.
- Biometric data (fingerprints, hand contour, iris ...)
- Genetic information (DNA)
- Offenses, condemnations, security measures
- Social security number (unless already authorized agencies)
- Assessments (reviews, comments) on the social problem of people.

Therefore, neither the social graph nor the present services provided manage any sensitive data.

7.2. Privacy guidelines for OASIS Services at Pilot Site 2: Italy

Within the scope of the OASIS project **Turin Province based in Italy** will test and implement services related to **2 types of applications**:

- **City Planning**
- **Mapping of territorial economic activities.**

The Data Protection Code relating to the protection of personal data (D. Lgs. 196/2003) guarantees **the free exchange of non-sensitive and non-personal data within the EU**. The services in use in the Italian Pilot work with data of public domain such as, names of the economic activities and destination of use of the territories of municipalities. Since the data are of public domain, an identification of the user of our two services is not mandatory.

7.3. Privacy guidelines for OASIS Services at Pilot Site 3: Bulgaria

Within the scope of the OASIS project **David Holding based in Bulgaria** will test and implement services related to **3 applications**:

- **Ushahidi**
- **Alternative Tourism Network**
- **User-centric citizen web portal for basic services**.

The services based on first two applications (i.e. Ushahidi and Alternative Tourism Network) do not handle personal data.

The third one will be an on-line portal type web application (developed by Open Wide partner to replace Capdemat), that runs in OASIS platform environment and provides access to more than 30 services offer by municipalities around the country running existing Archimed EDMS platforms.

Archimed application is complex system for document and workflow management that is a base for various e-services.

Currently David Holding install and support the Archimed system, but the **privacy and personal data handling** is responsibility of the organisations offering the services. They have the status of personnel data administrators.

When those services are accessed through OASIS the responsibilities depend on the service organisation:

- First case is when the control is transferred to e-service provider **before** entry of the personal data – here again David Holding resp. OASIS will not handle any personal data.

- Second case is if the personal data are requested and entered **within** OASIS portal service session. If the application is hosted in Bulgaria and David Holding is the operator there is no problem again, since David Holding have the status of Personal Data Administrator.

- If however the OASIS personal data are hosted in another country, e.g. France, and its laws are EU compliant, the platform manager/operator (Pole Numerique), must be formally represented in Bulgaria from legal point of view by an organisation, that has the status and is registered as a Personal Data Administrator. In our case this will be David Holding.

7.4. Privacy guidelines for OASIS Services at Pilot Site 4: Turkey

Within the scope of the OASIS project **EDMA based in Turkey** will test and implement services related to 2 types of applications:

- **Investment Promotion and Business Retention**
- **Data Collection from Public and Local Authorities.**

Turkish legislation **does not define an overarching framework for data protection**, thus generating a need for an omnibus regulation, which is mulled in the Draft Law on the Protection of Personal Data which mainly follows the EU Data Protection Directive No.95/46/EC. However, there are sector-specific and secondary regulations that are in force to secure personal data privacy. There's even no concrete definition for “personal data” with the exception of the “Regulation on Personal Data Processing and Protection at Telecommunication Sector” which is merely a secondary legislation under the Constitution and the Laws, Codes and Public Acts, and mainly concerns telecommunication service providers (broadband network, mobil communication etc.). It is fair to say that according to the ‘Medical Deontology Bylaw’ health condition is categorized as personal data.

Investment Promotion and Business Retention (INVPROM)

This application is to be used for promoting a region online and attracting foreign and domestic investment. It is a unique type of content manager, which allows service providers to feed in information and publish it online, with extra features such as searchable incentive schemes and angel investor - entrepreneur match making.

Users will be required to provide only their names, name of their companies, and e-mail addresses (EDMA don't collect data related to home address, age, family, friends, racial or ethnic origin, political and other opinions-beliefs, Social Security Number, sex, sexual orientation, private life, health condition, facial picture or other biometric data). Further to these information, it is fully up to the preference of the user to provide his/her company's contact information, annual volume of sales/operations, details about new proposed investment (size of investment, target sector, employment to be created, waste to be created, preferred sites). The user will be asked to read and accept the terms and conditions in a Disclaimer page (as explained in section 3.4.2), the content of which will be fed by the Service Provider.

Data Collection (DATAColl)

This application is to be used by Regional Planning Authorities for collecting information from Public Authorities (Regional offices, Provincial offices, Local Authorities, Central Authorities etc.). Regional Planner are often faced with the major problem of maintaining the stream of standardized information (data mining), which is normally scattered among different public bodies (Data Providers) in an unorganized or not up to the required arrangement in its default format.

All the data to be collected will be public metadata, which can be published and shared on public websites. This issue can be addressed in the agreement texts that could be signed between Data Collectors and Data Providers. Each Data Collector has to abide by the relevant laws and regulations governing the data they will collect using this application.

7.5. Privacy guidelines for OASIS Services at Pilot Site 5: Spain

Within the scope of the OASIS project **Blau Advisors based in Spain** will test and implement services related to **3 types of applications**:

- **A user-centric citizen web portal of basic services**
- **A software suit for the internal management of local public authorities**
- **Mapping of territorial economic activities.**

In the case of mapping of territorial economic activities where the information used is always public there is no specific need for the protection of the data.

For the other two services we need to identify different elements:

- **Consecution of explicit acceptance of the acquisition, treatment and storage of the personal data** made by the user prior to the submission of any data to the system. Due to that the first form including information that will be submitted to OASIS must have a disclaimer including the information and a check box accepting it. No transmission could be done with the check-box empty.

- **Consecution of explicit acceptance of the fact that the public body will ask for information related to the requester to other public bodies** in order to complete the request. If the user does not allow to it, then the citizen must provide this information. Previous to the moment of requesting this information to third parties, the user must fill in a form (or it could be in the initial one if it is possible) including a disclaimer including the information and a check box accepting it. Only for those users with the check box selected the public body will be able to ask for information on behalf of them.

- **Transmission of personal data specially protected.** All the information described in chapter as specially protected cannot be delivered to third parties (included OASIS platform) unless the citizen allows to it. Deliver also includes the transmission of personal data considered as

private to the datacore. In this case Spanish legal framework allows to make two actions: 1) To advise the citizen that information will be delivered to 3rd parties in case of need for the correct treatment of the request and afterwards to sign the correct agreement between the public body and the OASIS platform or 2) to mention explicitly the 3rd parties to the citizen in the moment of the begin of the request. It is easy and legal compliant the first mode.

8. Privacy Guidelines for high-risk services

This section presents some privacy guidelines that will need to be considered if the OASIS platform was to ever design and deploy high-risk services. Although the existing services selected for OASIS seem to be low-risk for privacy requirements and personal data, the aim of the OASIS platform is to be able to cope with the implementation of any kind of service.

According to the guide for protecting the confidentiality of the Personally Identifiable Information (PII) published by NIST [8], there is a need to protect (a) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (b) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Therefore, there is a need for authorities to identify these PII in order to protect them from misuse.

In the case of OASIS platform, the list of identified possible high-risk services and example PII fields are presented below:

- Payment Services
  - Handling of Financial Information: e.g. bank account number, credit card number
- Processing Sensitive Personal Data
  - Handling of Personal Data of Children: e.g.
  - Handling of Health Data: e.g. medical history

In terms of legal requirements, as per the Data Protection Directive 95/46/EC the data for these high risk services are deemed “**Special categories of personal data**” which refer to any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Therefore requires careful handling of such data and these sensitive data cannot be revealed to the service provider or allow for cross-border data transfers.

In terms of functional requirement, as per the guide published by NIST, it recommends that authorities are recommended that the PII confidentiality impact level to be set at least to moderate if a certain data field, such as SSN, is present [8]. Organisations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others.

Apart from being aware of these highly sensitive fields in the OASIS platform, it is also important to prevent access to these data by having in high levels of authentication. The recommendations for authentication of these high-risk services are based on one of the four levels of authentication derived from the international standards for electronic authentication guideline published by NIST [9].

It is highly recommended that the OASIS architecture integrates a Level 4 authentication system if and when the above listed high risk services are to be provided. **Level 4 requires “strong cryptographic authentication of all parties, and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used.”**

"The token secret shall be protected from compromise through the malicious code threat. Long-term shared authentication secrets, if used, shall never be revealed to any party except the Claimant and CSP; however session (temporary) shared secrets may be provided to Verifiers or RPs by the CSP. Strong, Approved cryptographic techniques shall be used for all operations including the transfer of session data. All sensitive data transfers shall be cryptographically authenticated using keys that are derived from the authentication process in such a way that MitM attacks are strongly resisted."

As highlighted this level of authentication is intended to provide the highest practical remote network authentication assurance.

Finally, although these guidelines presented are to be taken into consideration, it is important to note that there is no "one fits all" solution, so high privacy requirements would probably mean having in place various techniques to safeguards these information and additionally also use different authorization techniques, such as electronic identities instead of passwords.

9. Conclusions

The aim of this deliverable was to present a detailed set of privacy requirements that was derived from the data protection legislation for the OASIS architecture and its services. In the first iteration of privacy requirements identification, deliverable 1.31 presented the public services that were running in the cloud environment, based on the diversity of the Member States transpositions of the Directive and the Turkish legislation in force. As a result, the deliverable presented recommendations for OASIS that derived from the analysis of each service and the four national legislative contexts at the early stages of the project.

This deliverable is the second iteration of the privacy requirements analysis. This deliverable has provided a deeper and detailed evaluation of privacy requirements and personal data legislation with respect to the implemented OASIS architecture by having a particular focus on the nature of data that will be kept by the OASIS platform and by the public agencies that provide each e-service. The key conclusions derived from this deliverable are that:

- the amendments to the national legislations has had no major implications on the OASIS services since the submission of D1.31.
- the data core, social graph and authentication have been identified as the key elements of OASIS architecture that has presented some privacy concerns
- most of the public services still process data that are not sensitive personal data and hence low risk for information privacy exists.

This report has highlighted the proposed measures that have been taken by OASIS to address the privacy issues and reported any additional functional and legal guidelines that need to be addressed. As a result this deliverable has reported a detailed privacy analysis of the OASIS platform as whole and its services. Table 8 presents the privacy and functional requirements of the OASIS architecture for the pilot sites derived from the analysis of the architecture and the national legislations of the pilot sites.

Finally, the set of recommendations provided in this deliverable will help feed as input to the following deliverables:

- functional and legal requirements mainly listed in section 4.1 and 4.2 should be taken into account by Pole Numerique (OASIS platform manager) when finalising the contractual agreement with the chosen cloud provider (i.e. IPgarde).

- authentication recommendations mainly presented in section 5.4.2 will feed into D2.3 that reports the adapted solutions for user identification and authentication.
- the recommendations highlighted in section 7 for the services offered by each site should mainly feed into deliverables D3.5 which reports the governance of the OASIS architecture and the handling of data in the platform respectively.

OASIS Architecture		Processing of personal data	Privacy and Functional Requirements for the OASIS Architecture				
			Italy	France	Bulgaria	Turkey	Catalonia
Portal		√	No additional requirements if proper legal arrangements are set	**Main Portal**	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set
Data Core		√	**One instance of Data core due to legal requirements**	**One instance of Data core due to legal requirements**	No additional requirements if proper legal arrangements are set	Only holds business data and no personal information. No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set
Kernel	**Social Graph**	√	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set
	Authentication	√	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set	No additional requirements if proper legal arrangements are set
High Risk Services (Only applicable in the instance when requesting **special categories of data** such as health information etc.)		√ Personal data and special categories of personal data	Specify data controller, notify or ask permission from authority (based on national legislation), conduct risk analysis, implement security controls, pay particular attention to the guidelines for special categories of data (i.e health)	Specify data controller, notify or ask permission from authority (based on national legislation), conduct risk analysis, implement security controls, pay particular attention to the guidelines for special categories of data (i.e health)	Specify data controller, notify or ask permission from authority (based on national legislation), conduct risk analysis, implement security controls, pay particular attention to the guidelines for special categories of data (i.e health)	Specify data controller, notify or ask permission from authority (based on national legislation), conduct risk analysis, implement security controls, pay particular attention to the guidelines for special categories of data (i.e health)	Specify data controller, notify or ask permission from authority (based on national legislation), conduct risk analysis, implement security controls, pay particular attention to the guidelines for special categories of data (i.e health)

Table 8: Privacy and Functional Requirements of the OASIS architecture for the pilot sites

10. References

[1] A. Kronabeter and S. Fenz, “Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation,” in *Third International Conference, CloudComp 2012, Vienna, Austria, September 24-26, 2012,*, Vienna, Austria, 2012.

[2] ISO/IEC 29100:2011, “ Information technology-Security techniques-Privacy framework,” 2011. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45123. [Accessed 10 October 2013].

[3] W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” NIST - National Institute of Standards and Technology, Gaithersburg, 2011.

[4] The European Network and Information Security Agency (ENISA), “Cloud Computing Benefits, risks and recommendations for information security,” The European Network and Information Security Agency, EU, 2009.

[5] 95/46/EC, “Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF. [Accessed 10 October 2013].

[6] S. Gurses, C. Troncoso and C. Diaz, “Engineering Privacy by Design,” in *In Proceeding of Conference on Computers, Privacy & Data Protection (CPDP 2011)*, 2011.

[7] European Commission, “Opinion 2/2009 on the protection of children's personal data,” 2009. [Online]. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf. [Accessed 10 October 2013].

[8] E. McCallister, T. Grancy and K. Scarfone, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” NIST - National Institute of Standards and Technology, Gaithersburg, 2010.

[9] NIST; National Institute of Standards and Technology, “Electronic Authentication Guideline,” 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf. [Accessed 2013 October 2013].