ECOBULK

Circular Approach for Eco-Composite Bulky Product

GA NUMBER: 730456

D1.5 DATA MANAGEMENT PLANT

Report Name:	**ECOBULK-D1.5-WP1-30112017.doc**
Version Number:	**2**
Document Number:	**D1.5**
Due Date for Deliverable:	**M6**
Actual Submission date:	**30/11/2017**
Lead Beneficiary:	**Exergy Ltd**

Start date: 01/06/17. Duration: 48 Months

DOCUMENT CONTROL PAGE

Author	Fernando Sanahuja Diago
Version number	02
Date	30/11/2017
Modified by	
Comments	
Status	✓ Delivered Accepted
Action requested	To be revised Deadline for action: No action

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730456

EXECUTIVE SUMMARY

This document describes the Initial Data Management Plan (DMP) for the ECOBULK project, funded by the EU's Horizon 2020 Programme under Grant Agreement number 730456. The DMP provides an analysis of the main elements of the data management policy that will be used throughout the ECOBULK project by the project partners, with regard to all the datasets that will be generated by the project.

The DMP will present in detail only the procedure for the management of datasets created during the lifetime of the project and describes the key data management principles, notably in terms of data standards and metadata, sharing, archiving and preservation.

The format of the plan follows the Horizon 2020 template and its content has been guided by the advice from the UK Data Service.

DOCUMENT INFORMATION

Title	ECOBULK-WP1-D1.5-EXE-20171130_V02
Lead Beneficiary	Exergy Ltd (EXE)
Contributors	Exergy Ltd (EXE)
Distribution	Public
Report Name	Data Management Plan

DOCUMENT HISTORY

Date	Version	Prepared by	Organization	Notes
15/11/2017	V01	Fernando Sanahuja	Exergy Ltd (EXE)	
30/11/2017	V02	Fernando Sanahuja	Exergy Ltd (EXE)	

ACKNOWLEDGEMENTS

The work described in this document was subsidised by the European Community Horizon 2020 through the Grant Agreement Number 730456.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

One of the fundamental elements of a good data management is the Data Management Plan (DMP), which defines the principles and procedures of data collection, processing and generation, composing the data management life cycle of a Horizon 2020 project. In order to make research data FAIR (findable, accessible, interoperable and re-usable) and ensure it is soundly managed, a DMP should include information on:

- the handling of research data during and after the end of the project
- what data will be collected, processed and/or generated
- which methodology and standards will be applied
- whether data will be shared/made open access and
- how data will be curated and preserved (including after the end of the project).

In Horizon 2020, the Commission has launched a flexible pilot for open access to research data (ORD pilot). The pilot aims to improve and maximise access to and re-use of research data generated by Horizon 2020 projects, taking into account the need to balance openness and protection of scientific information, commercialisation and IPR, privacy concerns, security and data management and preservation questions.

All projects participating in the extended ORD pilot are required to have a DMP, in which they will specify what data will be open: detailing what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved[1].

The present Data Management Plan (DMP) for the ECOBULK project has been prepared by following the considerations included in the EU template of the "*Guidelines on Data Management in Horizon 2020*" (http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oadata-mgt_en.pdf).

[1] http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

2. DATA COLLECTION PROCEDURES

The development of the DMP for ECOBULK project will permit the consortium partners to deal with all issues regarding data management. Even though the DMP is a Deliverable due on Month 6 (D.1.5), it will be a live document throughout the project. This initial version needs to be updated over the course of the project whenever significant changes arise, such as (but not limited to) new data, changes in consortium policies and/or changes in consortium composition and external factors.

The consortium will comply with the requirements of Directive 95/46/EC 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.

Type of data, storage, recruitment process, confidentiality, ownership, management of intellectual property and access: The Grant Agreement and the Consortium Agreement are to be referred to for these aspects, particularly Articles 18, 23a, 24, 25, 26, 27, 30, 31, 36, 39 and 52 and "Annex I – Description of the Action" of the Grant Agreement. The Grant Agreement was signed on 02/05/2017 while the Consortium Agreement was set into force on 24/05/2017. The procedures to be implemented for data collection, storage, access, sharing policies, protection, retention and destruction will be according to the requirements of the national legislation of each partner and in line with the EU standards.

The Steering Committee of the project will also ensure that EU standards are followed. Regarding the issue of informed consent for all survey procedures, all participants will be provided with a Participant Information Sheet and Consent Form to provide informed consent. The default position for all data relating to residents and staff will be anonymous.

The responsible partners will assure that the EU standards regarding Data Management are fulfilled. Each partner will proceed with the survey according to the provisions of the national legislation that are adjusted according to the respective EU Directives for Data Management.

a) The consortium will preserve the right to privacy and confidentiality of data of the participants in the surveys by providing all participants to the survey with two documents: The Participant Information Sheet and the Consent Form. These documents will be sent electronically and will provide information about how the answers will be used and what is the purpose of the survey. The participants will be assured that their answers will be used only for the purposes of the specific survey. The voluntary character of participation will be stated explicitly in the Consent Form.

b) The consortium will examine before conducting the survey – following the requirements of the national legislation in line with the EU standards - whether the proposed data collection requires special local/national ethical/legal permission.

c) The recruitment process to be followed by the consortium for the engagement of stakeholders (including inclusion/exclusion criteria for all the surveys) will be transparent and such criteria will be included and explained in the Participant Information Sheet. Participants to the survey will be invited by each partner by email. The third parties that will be invited to participate in the survey will have no role in ECOBULK and no professional relationship with the consortium. The consortium will also examine whether personal data will be collected and how to secure the confidentiality in such a case.

3. OVERALL DATASET STRUCTURE

The Data Management Plan will present in detail only the procedures of creating 'primary data' (data not available from any other sources) and of their management.

4. MANAGEMENT PLANS FOR INDIVIDUAL DATASETS

This section will develop as the project progresses, and reflects the current status within the consortium about the primary data that will be produced.

Data set reference and name	ECOBULK platforms, surveys and interviews
Data set description	The Database Management System will be developed building on partners' specific and validated expertise and will enable the collection, analysis, and store of performance and operational data obtained from product designs, manufacturing, services, logistics and (re-)manufacture, and recycle processes as well as data for material stream flows, composition and effectiveness of technologies for material production. Surveys and structured interviews will be conducted to end-users and other stakeholders (e.g. manufacturers, consumers) of the DEMO activities to obtain social, economic and environmental information related to the design of the products. Customer satisfaction surveys are also envisaged. These activities are planned in WP2 and WP8. An online stakeholder platform will be developed (WP6) to create a direct engagement between different actors (designers, manufactures, distributors, collectors) and end users of the ECOBULK solutions. Therefore, a report describing the informed consent procedures will be delivered.
Origin of data	Data collection will be carried out with the aim to obtain social information for the product design as well as behaviour and feedback from the end users in DEMO activities.

	During the activities developed in WP2, information regarding social, environmental and economic aspects will be collected as well as the satisfaction and feedback from end user and designers. Likewise, the bidirectional platform (WP6) will enable identification of consumption patterns, customization and development of value-added goods. Only basic personal information related to the end users and other stakeholders will be collected. Sensitive personal information (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction) will not be collected during the survey process. The information will be related to economic, environmental and social aspects related to the design of products, including several issues across the entire process (material, employment, information, etc).
Scale	Scale of the still questionnaires still needs to be defined.
Standards and metadata	The data from the questionnaires shall be held in transcript form in accessible file formats such as .xls (Excel), .accdb (Access) or .doc (Word). Existing suitable standards in the relevant discipline shall be adhered to. The type of metadata that will be created is to be confirmed.
Data collection procedures	Information will be gathered through surveys and interviews, and will be stored in digital format at least until the project finalisation. Information might be potentially gathered from the online end-user and stakeholders' platform too.

	Consent from the surveyed people will be obtained during the activity by accepting previous set terms and conditions. In the case of the surveys, the respondent needs to accept the privacy policy on how the Consortium will handle and process the data. The respondents will be required to accept the surveys' policy by agreeing the privacy police check-box. Likewise, they will decide whether they want to subscribe to the ECOBULK's newsletters through accepting or declining the corresponding checkbox. The privacy policy will be also provided to the respondents of the phone and direct interviews, in the former case it will be read and the explicit consent of the respondents will be required in order to continue with the survey, and in the latter case the privacy policy will be the first document handle to the respondents. An online link where that privacy policy and other relevant survey related information can be found (e.g. data process and storage, purpose of the surveys, where do they find the statistical final results, etc.) will be also provided.

Table 1 - Data set for ECOBULK platform

5. DATA SHARING

The data sharing procedures are the same across the datasets and are in accordance with the Grant Agreement. Table 2 outlines the project access procedures and rights in relation to the data gathered through the ECOBULK project.

Access Procedures	Regarding the digital research data generated in the action ('data'), the beneficiaries must: (a) deposit in a research data repository and take measures to make it possible for third parties to access, mine, exploit, reproduce and disseminate — free of charge for any user — the following: (i) the data, including associated metadata, needed to validate the results presented in scientific publications as soon as possible; (ii) other data, including associated metadata, as specified and within the deadlines laid down in the 'data management plan' (see Annex 1 of Grant Agreement); (b) provide information — via the repository — about tools and instruments at the disposal of the beneficiaries and necessary for validating the results (and — where possible — provide the tools and instruments themselves). This does not change the obligation to protect results in GA Article 27, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply. As an exception, the beneficiaries do not have to ensure open access to specific parts of their research data if the achievement of the action's main objective, as described in Annex 1 of the GA,

	would be jeopardised by making those specific parts of the research data openly accessible. In this case, the data management plan must contain the reasons for not giving access. In accordance with Grant Agreement, data must be made available upon request, or in the context of checks, reviews, audits or investigations.
Access rights	To exercise access rights, this must first be requested in writing ('request for access'). 'Access rights' means rights to use results or background under the terms and conditions laid down in the Grant Agreement. Waivers of access rights are not valid unless in writing. Unless agreed otherwise, access rights do not include the right to sub-license. The beneficiaries must give each other access — on a royalty-free basis — to background needed to implement their own tasks under the action, unless the beneficiary that holds the background has — before acceding to the Grant Agreement —: (a) informed the other beneficiaries that access to its background is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel), or (b) agreed with the other beneficiaries that access would not be on a royalty-free basis. The beneficiaries must give each other access — under fair and reasonable conditions — to background needed for exploiting their own results, unless the beneficiary that holds the background has — before acceding to the GA — informed the other beneficiaries that access to its background is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel).

	'Fair and reasonable conditions' means appropriate conditions, including possible financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged. Requests for access may be made — unless agreed otherwise — up to one year after the period set out in Article 3 of the GA. Unless otherwise agreed in the consortium agreement, access to background must also be given — under fair and reasonable conditions (see above; Article 25.3) and unless it is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel) — to affiliated entities18 established in an EU Member State or 'associated country'19, if this is needed to exploit the results generated by the beneficiaries to which they are affiliated. Unless agreed otherwise (see above; Article 25.1), the affiliated entity concerned must make the request directly to the beneficiary that holds the background. Requests for access may be made — unless agreed otherwise — up to one year after the period set out in Article 3. Access rights for third parties is not applicable. If a beneficiary breaches any of its obligations, the grant may be reduced (see Article 43 in the GA). Such breaches may also lead to any of the other measures described in Chapter 6 of GA.

Table 2 - Access procedures and rights

5.1. EXPLOITATION AND DISSEMINATION

Each ECOBULK partner must, in accordance with Article 28 of the Grant Agreement, take measures to ensure the 'exploitation' of its results, up to four years after the period set out in Article 3 (48 months). The ECOBULK partners can use a variety of methods for this including:

- Using them in further research activities (outside the action);
- Developing, creating or marketing a product or process;
- Creating and providing a service, or
- Using them in standardization activities.

This does not change the security obligations in Article 37, which still apply.

Each ECOBULK partner must also 'disseminate' its results in accordance with Article 29 of the GA. The partner must give advance notice to the other partners of at least 45 days. Each partner must also ensure open access to all peer-reviewed scientific publications relating to its results. As per Article 29.2, the partners must:

- As soon as possible and at the latest on publication, deposit a machine-readable electronic copy of the published version or final peer-reviewed manuscript accepted for publication in a repository for scientific publications; Moreover, the beneficiary must aim to deposit at the same time the research data needed to validate the results presented in the deposited scientific publications.

- Ensure open access to the deposited publication — via the repository — at the latest:
    - On publication, if an electronic version is available for free via the publisher, or o Within six months of publication (twelve months for publications in the social sciences and humanities) in any other case.
    - Ensure open access — via the repository — to the bibliographic metadata that identify the deposited publication. The bibliographic metadata must be in a standard format and must include all of the following:

- the terms "European Union (EU)" and "Horizon 2020";
- the name of the action, acronym and grant number;
- the publication date, and length of embargo period if applicable, and
- a persistent identifier.

6. ARCHIVING & PRESERVATION

Providing information and keeping records	Data will be properly stored and protected in order to allow for the validation of the findings, further data analysis, compliance with funding requirements, etc. Online collected data will be stored on a platform managed by the tasks leaders and accessible only to partners directly involved with the tasks. Furthermore, the online data will be downloaded and saved in electronic format along with the data collected through phone and direct face to face interviews. In the eventually of surveys being completed on paper, the information will be digitalized. Data will be stored in the specific hard disk and online cloud as security copy as long as the survey activity is ongoing. The data will be managed directly by the Task Leader and only accessible to relevant partners. The data will be analysed and kept for follow-up actions until the relevant reports are completed and delivered, afterwards the information will be destroyed. All electronic and physical data will be destroyed and data store on any online secured platform will be deleted. The retention of the data collected could last until one year after the end of the project's life. The beneficiaries must provide — during implementation of the action or afterwards and in accordance with Article 41.2 of GA — any information requested in order to verify eligibility of the costs, proper implementation of the action and compliance with any other obligation under the Agreement.

Each beneficiary must keep information stored in the Participant Portal Beneficiary Register (via the electronic exchange system; see Article 52 of GA) up to date, in particular, its name, address, legal representatives, legal form and organisation type.

Each beneficiary must immediately inform the coordinator — which must immediately inform the Agency and the other beneficiaries — of any of the following:

(a) events which are likely to affect significantly or delay the implementation of the action or the EU's financial interests, in particular:
    (i) changes in its legal, financial, technical, organisational or ownership situation or those of its linked third parties and
    (ii) changes in the name, address, legal form, organisation type of its linked third parties;
(b) circumstances affecting:
    (i) the decision to award the grant or
    (ii) compliance with requirements under the Agreement.

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43 of GA). Such breaches may also lead to any of the other measures described in Chapter 6 of GA.

The beneficiaries must — for a period of five years after the payment of the balance — keep records and other supporting documentation in order to prove the proper implementation of the action and the costs they declare as eligible.

They must make them available upon request (see Article 17 of GA) or in the context of checks, reviews, audits or investigations (see Article 22 of GA).

	If there are on-going checks, reviews, audits, investigations, litigation or other pursuits of claims under the Agreement (including the extension of findings; see Articles 22 of GA), the beneficiaries must keep the records and other supporting documentation until the end of these procedures. The beneficiaries must keep the original documents. Digital and digitalised documents are considered originals if they are authorised by the applicable national law. The Agency may accept non-original documents if it considers that they offer a comparable level of assurance. The beneficiaries must keep records and other supporting documentation on scientific and technical implementation of the action in line with the accepted standards in the respective field. The beneficiaries must keep the records and documentation supporting the costs declared, in particular the following: (a) for actual costs: adequate records and other supporting documentation to prove the costs declared, such as contracts, subcontracts, invoices and accounting records. In addition, the beneficiaries' usual cost accounting practices and internal control procedures must enable direct reconciliation between the amounts declared, the amounts recorded in their accounts and the amounts stated in the supporting documentation; (b) for unit costs: adequate records and other supporting documentation to prove the number of units declared. Beneficiaries do not need to identify the actual eligible costs covered or to keep or provide supporting documentation (such as accounting statements) to prove the amount per unit. In addition, for direct personnel costs declared as unit costs calculated in accordance with the beneficiary's usual cost accounting practices, the beneficiaries must keep adequate records and documentation to prove that the cost accounting practices used comply with the conditions set out in Article

	6.2, Point A, of GA. The beneficiaries and linked third parties may submit to the Commission, for approval, a certificate (drawn up in accordance with Annex 6 of GA) stating that their usual cost accounting practices comply with these conditions ('certificate on the methodology'). If the certificate is approved, costs declared in line with this methodology will not be challenged subsequently, unless the beneficiaries have concealed information for the purpose of the approval. (c) for flat-rate costs: adequate records and other supporting documentation to prove the eligibility of the costs to which the flat-rate is applied. The beneficiaries do not need to identify the costs covered or provide supporting documentation (such as accounting statements) to prove the amount declared at a flat-rate. In addition, for personnel costs (declared as actual costs or on the basis of unit costs), the beneficiaries must keep time records for the number of hours declared. The time records must be in writing and approved by the persons working on the action and their supervisors, at least monthly. In the absence of reliable time records of the hours worked on the action, the Agency may accept alternative evidence supporting the number of hours declared, if it considers that it offers an adequate level of assurance. As an exception, for persons working exclusively on the action, there is no need to keep time records, if the beneficiary signs a declaration confirming that the persons concerned have worked exclusively on the action. For costs declared by linked third parties (see Article 14 of GA), it is the beneficiary that must keep the originals of the financial

	statements and the certificates on the financial statements of the linked third parties. If a beneficiary breaches any of its obligations under this Article, costs insufficiently substantiated will be ineligible (see Article 6 of GA) and will be rejected (see Article 42 of GA), and the grant may be reduced (see Article 43 of GA). Such breaches may also lead to any of the other measures described in Chapter 6 of GA.
Length of retention	The retention of the data collected could last until one year after the end of the project's life.

7. LEGAL FRAMEWORK FOR PRIVACY PROTECTION

ECOBULK aims at implementing a new economy model for composite products in automotive, furniture and building component industrial sectors with high potential of cross-sectorial replicability and transferability by directly addressing and demonstrating key stages along the entire circular setup. That objective is meant to be achieved, among other measures, by developing a User and Stakeholder platform in the cloud for carrying out some activities of the project.

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

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

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

The use cases for ECOBULK platform in general consist of gathering data and information about the technologies, demonstration sites and other aspects that will need to be specified for the proper development of the project, which imply transfer/exchange of data/information. Any action that takes place in such a service environment can potentially raise privacy issue, which could be addressed not only through technology but also through the procedures in place. Privacy issues also arise in platform development projects where testing and pilot execution phase exists, as collection of information about individuals, public entities and private organizations will be required.

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

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

7.1. EU legal framework for privacy protection

Privacy is enabled by protection of personal data. According to Data Protection Directive (95/46/EC) of the EC, personal data "means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one of more factors specific to his physical, physiological, mental, economic, cultural or social identity".

The same Directive also defines personal data processing as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

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

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

- Directive 95/46/EC (Data protection Directive)
  The Directive regulates the processing of personal data regardless of whether such processing is automated or not. The principle is that personal data should not be processed at all, except when certain conditions are met.
    - Article 6(b): Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."

- Article 7 defines criteria for making personal data processing legitimate:
  - the data subject has given his consent
  - processing is necessary for the performance of or the entering into a contract the data subject is party
  - processing is necessary for compliance with a legal obligation the controller is subject
  - processing is necessary in order to protect the vital interests of the data subject
  - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
  - processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

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

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

- Article 5 Confidentiality of the communications

  - Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping,

storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

- Paragraph 1 shall not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

- Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

- Directive 2009/136/EC (Cookie Directive)

  This Directive amended Directive 2002/58/EC, requiring end user consent to the storing of cookies on their computer. Cookies are hidden information exchanged between an Internet user and a web server stored in a file on the user's hard disc. They can be used to monitor Internet activities of the user.

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

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

7.2. Accessibility and "easy-to-use" principle

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

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

The EU Law related to the issue is the following:

- Charter of Fundamental rights of the EU (Article 21- non-discrimination)
    - Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

- Digital Agenda for Europe COM (2010) 245 final

    - It is essential to educate European citizens to use ICT and digital media and particularly to attract youngsters to ICT education

- There is also need for concerted actions to make sure that new electronic content is also fully available to persons with disabilities. In particular, public websites and online services in the EU that are important to take a full part in public life should be brought in line with international web accessibility standards [Web Content Accessibility Guidelines (WCAG) 2.0.]. Moreover, the UN Convention on the Rights of persons with disabilities contains obligations concerning accessibility.

7.3. Data security

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

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

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

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

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

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

7.4. National frameworks

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

Three municipalities -demosites- will validate and demonstrate the end user and stake holder platform by building on existing recycling and reuse programs; Exergy-Warwickshire council (**United Kingdom**)- Recycle for Warwickshire, Lipor (**Portugal**), FCBA (**France**).

7.4.1. UNITED KINGDOM

The ECOBULK project will develop demonstration activities in a demosites in the United Kingdom: Warwickshire council.

Data collection procedures in the UK are legislated for by the Data Protection Act (DPA). However, this legislation regulates only the use of "personal data". As such it is only of relevance to the project where data collected can be defined as "personal data". The DPA defines "personal data" as follows:

Personal data *means data which relate to a living individual who can be identified –*

(a) *from those data, or*
(b) *from hose data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*

According to the above definition, applicability of the DPA to the project would depend on the monitoring systems installed. Thus, the selection of the monitoring systems should be undertaken to avoid the potential to identify living individuals If it is possible to identify living individuals, including when combining monitoring data

with information which is likely to come into possession of the project, the DPA would need to be adhered to.

Incidentally, images of people (e.g. from CCTV systems) are covered by the DPA and thus, collection of images of people in the project should be avoided or further actions should be taken to ensure compliance with the DPA.

Personal Data Protection British regulation

- The Information Commissioner's Office (ICO)
- UK Data Protection Act 1998
- The Privacy and Electronic Communications (EC Directive) Amendment Regulations 2011
- Human Rights Act 1998 ("HRA")
- Regulation of Investigatory Powers Act 2000 ("RIPA")

7.4.2. PORTUGAL

Portuguese national frameworks are discussed here from the Portuguese Law and regional Law perspectives including Local City Councils decisions related to public participation, electronic communication, e-Government policies, and personal data protection.

Different regulatory topics analysed and identified in Portuguese pilot use-cases based on personal data protection are as follows:

Personal Data Protection Portuguese Regulation

- The Data Protection Act (DPA) defines personal data as "any information relating to an identified or identifiable natural person, regardless of its support, including sound and image". A natural person is deemed to be identifiable when he/she can be directly or indirectly identified, including by reference to an identification number or to one or more features that are specific to his/her physical, physiological, mental, economic, cultural or social identity.

- The provisions of Directive 95/46/EC on data protection (Data Protection Directive) were implemented into Portuguese law through Law 67/98 of 26 October 1998 (Data Protection Act). The fundamental principles and guarantees on personal data protection are also set out in the Portuguese Constitution (Article 35 on the use of computerised data).

- Sectorial laws or regulations include the rules applicable to the electronic communication (telecom) sector as contained in Law 41/2004 of 18 August 2004, which implemented Directive 2002/58/EC on the protection of privacy in the electronic communications sector (E-Privacy Directive) (as amended by Law 46/2012 of 29 August 2012 implementing Directive 2002/22/EC on universal service and users' rights (Universal Service Directive) and Regulation (EU) 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC).

- The provisions of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive) (amending the E-Privacy Directive) have also been implemented into Portugal through Law 32/2008 of 17 June 2008 on the retention and transfer of personal data for the purposes of the investigation, detection and prosecution of serious crime by competent authorities.

The Portuguese demosite will apply their own checking mechanisms to sustain ethics and privacy issues during the ECOBULK project.

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

7.4.3. FRANCE

The French DPA was recently substantially amended by Law No 2016-1321 for a Digital Republic dated 7 October 2016 (Digital Republic Law). In part the amendment was made to prepare for Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), due to come into force on 25 May 2018.

The French Data Protection Authority (Commission Nationale de l' Informatique et des Libertés) (CNIL) supervises enforcement of the DPA and frequently issues decisions and guidelines on it. See box, Regulator details.

Personal Data Protection French regulation

There are a bundle of laws and regulations relating to personal data protection regulating specific sectors, including:

- Act No 78-17 on Information Technology, Data Files and Civil Liberties dated 6 January 1978 (DPA). This act was modified to implement Directive 95/46/EC on data protection (Data Protection Directive).
- Decree No 2005-1309 of 20 October 2005.
- Postal and Electronic Communications Code (*Articles L 34 et seq and Articles R 10 et seq*) (regulating online electronic communication services to the public).
- Property Code (*Article L 212-3*) (on the retention of personal data contained in public archives).

7.5. Privacy Protection Issues in pilot scenarios

Privacy protection issues in the pilot countries have been identified by pilot partners and they have been considered according to the use cases of ECOBULK platform and the issues that may arise. Table 3 summarizes these issues as follows:

Transaction/Use case, stakeholders involved, data/information exchange	**Issue that can arise**
Submitting petition	Virus can affect the system & protection of submitted content regarding the petition
E-government services in general	Accessibility and protection of submitted information
Usage of personal data in electronic transaction (uploading documents, submitting forms with personal information etc.)	Protection of personal data, commercial confidentiality, protection of intellectual property
Administrative policy making and participation process, led electronically, affecting the public interest	Transparency issues, Democratic Electronic Participation
Electronic Data Usage (Uploading, exchanging documents, GIS data etc.)	Security of Information and Data (Personal Data, Administrative Data) Accessibility Rights to the Government Services electronically Administrative Procedures (Stakeholders Requests, Administrative Decisions, Submittals and Transmittals complying the Deadlines) Liabilities arises due Data Usage and Storage (Industrial and Intellectual Property Rights, Protection against Espionage)
Personal and Sensitive Data Management	Misuse of personal and sensitive data
Personal and Sensitive Data Management	Data usage for private/market purposes
Hackers attacking the system	Privacy protection issues

Table 3 - Privacy Protection Issues that can raise in pilot scenarios

8. CLOUD COMPUTING IMPACT ON PRIVACY PROTECTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. ENVIRONMENT PROTECTION

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

- The right of partners to access to information;
- The right of partners to participate in decisions about the environment;
- The right to access justice when the previous two rights are violated.

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

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

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

10. ECOBULK PLATFORM DATA PROTECTION GUIDELINES

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

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

A crucial aspect to be considered in this context is the platform development and the data privacy, which can trigger a number of data protection risks, mainly a reduced control over personal data as well as insufficient information with regard to how,

where and by whom the data is being processed/sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider.

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

- Minimization: ECOBULK procedures in the cloud should only handle minimal data about users.

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

- Consent: Consents have to be handled allowing the users to agree the transmission and storage of sensitive data. The consent text included in the interface should specify which data will be stored, who they will be transmitted to and for which purpose for the sake of transparency. The consent legal text must be customized for each pilot country with references to the local legislation that applies.

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

- Purpose specification and limitation: personal data must be collected just for the specified purposes of the participation process and not further processed in a way incompatible with those purposes. So not only the authority offering the service must guarantee that personal data are not processes for purposes not compatible with the original ones, but it must be ensured that personal data are not (illegally) processed for further purposes by the cloud provider or one of his subcontractors.

So, the applicant and other involved stakeholders, when they register into the system, have to receive a legal note specifying this.

- Erasure of data: personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Personal data that are not necessary any more must be erased or truly anonymized. If this data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be blocked. The cloud client should make sure that the cloud provider ensures secure erasure and that the contract between the provider and the client contains clear provision for the erasure of personal data. The same holds true for contracts between cloud providers and subcontractors.

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

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

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

- Security: Encryption of personal data should be used in all cases when "in transit" and when available to data "at rest". Communications between cloud provider and client as well as between data centres should be encrypted. Remote administration of the cloud platform should only take place via a secure communication channel.

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

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

10.1. ECOBULK Technical Approach

The technical solution set-up for the ECOBULK has taken into due consideration the recommendations drafted in this document and these will be implemented in order to minimize its impact in terms of privacy and confidentiality of personal data. This section of the deliverable illustrates the technical choices made with respect to these issues.

The ECOBULK project uses a number of security policies and rules to ensure the confidentiality, integrity and availability of electronic information captured, stored, maintained, and used. It has been provided authentication mechanisms and policies to assure authorized access to the data, the generation, maintenance and transmission of strong passwords. The ECOBULK platform will be hosted on a secure data centre infrastructure, which is controlled by the coordinator and is designed considering the cloud computing recommendations and technical. It provides an extremely scalable, highly reliable platform that enables users to deploy applications and data quickly and securely.

10.2. Protection of Personal Data

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

All activities will be carried out ensuring the ethical principles in accordance with Directive 95/46/EC of the European Parliament, about the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as DIRECTIVE 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, as modified by Directive 2009/136/EC. All national data protection and privacy laws for pilot countries will be also followed.

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

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

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

10.3. Personalized service and anonymous aggregation of user choices

Personalized services will be offered on the basis of registered user profiles that will be stored in the application server, deployed at a data centre controlled by the coordinator, and accessible only by authorized personnel. No passwords will be stored (only hashes) and therefore the personal profile information (including name, email, preferred topics and voting history) will be only accessible by the registered user. User registration, authentication and data access will be implemented according to state of the art security practices and standards.

10.4. Ethics Approval

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

10.5. Collection and/or processing of personal data for research procedures

The project performs and will perform user studies and tests during its research and evaluation stages. For the conduction of the user studies no personal sensitive data will be required. Following the best practice for ethics in Human-Computer Interaction, any personal (but not sensitive) data collected during the user evaluations will be anonymized or at least pseudonymized and used for the purposes of the project. The data may include personal information about the user such as: first name, surname, email address, phone number, postal address, date of birth, interests, posts, likes, comments, location, images, or relations to other users. They will not include

sensitive personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction).

The participation is voluntary and informed consent is collected from each individual user. In addition, an Information Sheet will be provided to each contacted individual, informing them about the scope of the research and where additional information can be sought.

10.6. Procedures for data collection, storage, protection, retention and destruction

The general framework by which data collection, storage, protection, retention and destruction is performed according to EU legislation, directives and opinions is laid out in details in Sections 10.2, 10.3, 10.4 and 10.5. Below it is presented specific policies that implement the privacy recommendations in the project platform and website. Each partner will comply with their national and EU data protection law, including notification of their national Data Protection Authority if necessary under their national law, when processing the personal data of the project applications users or any other personal data processed in the context of the project.

Each partner will provide precise information on what type of personal data they process concerning the project applications users, how it is processed and which data-flows they enable. Each partner will also provide an email address to be contacted in case a user wants to withdraw his/her consent for processing his/her personal data.

All parties shall carry out a personal information assurance risk assessment from their own context concerning their own collection, storage and/or processing of personal data, prior to the collection of personal data, and at any point through the operation of the system where there is a relevant change. Such a risk assessment shall follow information assurance principles and each partner is liable for inappropriate security at its own premises.

In terms of data retention and destruction, data will be deleted or fully anonymized as soon as the relevant scientific purpose as stated in the DoW is fulfilled. Regarding data processing, the collected data will be immediately pseudonymized and aggregated, and the original data will not be stored whatsoever.

10.7. Non-EU countries

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

10.8. Right to be forgotten and to erasure

Pilot users will have the right to obtain the erasure of personal data relating to them and the abstention from further dissemination of such data according to the General Data Protection Regulation. They will be informed about this right in the information sheets. Applications for erasure of data will be carried out without delay. In case the personal data has been made public, the consortium will take all reasonable steps, including technical measures, to inform third parties that are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data.

A procedure for exercising the right to be forgotten and to erasure will be provided, and will include appointment of a data protection manager, checking the validity of the request, identifying data which should be erased, monitoring the erasure process, and informing the pilot user.

11. CONCLUSION

D1.5. Data Management Plan has detailed EU level and national frameworks for handling legal and data protection issues. This deliverable aimed to identify key issues that can arise throughout the life of the ECOBULK project, considering aspects specific in each End-User and Stakeholder platform pilot country (United Kingdom, Portugal and France) and generally valid at the EU level.

This deliverable first investigated corresponding European directives including Data Protection Directive, e-Privacy Directive and Cookie Directive with the support of all national frameworks of pilot countries (United Kingdom, Portugal and France). Regarding the issues and regulatory frameworks analysed, guidelines and the technical approach for the ECOBULK platform are provided for the use of all partners and other Work Packages. Guidelines and the ECOBULK technical approach include solutions for the collection, processing and protection of personal data, personalized service and anonymous aggregation of user choices, procedures for data collection, storage, protection and retention of data, monitoring component and non-EU countries involvement.

The research conducted in this deliverable includes several important aspects of privacy & data protection from EU and national regulatory framework and technical perspectives. The guidelines in the deliverable will be a reference for technical and pilot partners of the ECOBULK platform both during the implementation and execution phase, and also for the exploitation of the platform which the consortium expect the deliverable to reach a wider audience of policy makers and researchers for further projects.

REFERENCES

1. "Guidelines on Data Management in Horizon 2020" (http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf).
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995
3. (EC) No 251/2005 of 11 March 2005 on the European Charter for Researchers and on a Code of Conduct for the Recruitment of Researchers (OJ L 75, 22.03.2005, p. 67), the European Code of Conduct for Research Integrity of ALLEA (All European Academies) and ESF (European Science Foundation) of March 2011. (http://www.esf.org/fileadmin/Public_documents/Publications/Code_Conduct_ResearchIntegrity.pdf)
4. Directive 95/46/EC on protection of personal data (Data Protection Directive)
5. Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)
6. Directive 2009/136/EC (Cookie Directive)
7. Act No 78-17 on Information Technology, Data Files and Civil Liberties dated 6 January 1978 (DPA). This act was modified to implement Directive 95/46/EC on data protection (Data Protection Directive).
8. Decree No 2005-1309 of 20 October 2005.
9. Postal and Electronic Communications Code (Articles L 34 et seq and Articles R 10 et seq) (regulating online electronic communication services to the public).
10. Property Code (Article L 212-3) (on the retention of personal data contained in public archives).
11. Law No 2016-1321 for a Digital Republic dated 7 October 2016 (Digital Republic Law)
12. Information Society Code (917/2014) (ISC)
13. Act on the Protection of Privacy in Electronic Communications (516/2004)
14. Act on the Protection of Privacy in Working Life (759/2004) (WPA)

15. Credit Data Act (527/2007) (CDA)
16. Act on the Status and Rights of a Patient (785/1992)
17. Act on Openness of Government Activities (621/1999)
18. Decree on Openness of Government Activities (1030/1999)
19. The Information Commissioner's Office (ICO)
20. Directive 95/46/EC on data protection
21. Portuguese Law 67/98 of 26 October 1998 (Data Protection Act)
22. Law 41/2004 of 18 August 2004, rules applicable to the electronic communication (telecom) sector
23. Directive 2002/58/EC on the protection of privacy in the electronic communications sector (E-Privacy Directive)
24. Law 46/2012 of 29 August 2012 implementing Directive 2002/22/EC on universal service and users' rights (Universal Service Directive)
25. Regulation (EU) 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC.
26. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive) (amending the E-Privacy Directive)
27. Law 32/2008 of 17 June 2008 on the retention and transfer of personal data for the purposes of the investigation, detection and prosecution of serious crime by competent authorities.
28. UK Data Protection Act 1998
29. The Privacy and Electronic Communications (EC Directive) Amendment Regulations 2011
30. Human Rights Act 1998 ("HRA")
31. Regulation of Investigatory Powers Act 2000 ("RIPA")
32. The Federal Act on Data Protection (FADP)

33. Ordinance to the Federal Act on Data Protection (OFADP).

34. http://uk.practicallaw.com

35. Dr. M.Serdar Yümlü, Caner Tosunoğlu, İbrahim Acar, Gonca Kara Demir, " Guidelines for handling ethical, legal issues, and data protection", STEP project, Societal and political engagement of young people in environmental issues, 2015.

36. HERON (No: 649690): Deliverable D.2.6, "Data Management Plan". Oxford Brookes University and Università Commerciale Luigi Bocconi, 2015.