Horizon 2020 Grant Agreement No 809965
Contract start date: July 1st 2018, Duration: 30 months

LAMBDA Deliverable 1.7
Data Management Plan

Due date of deliverable: 31/12/2018
Actual submission date: 28/12/2018

Revision: Version 1.0

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme, H2020-WIDESPREAD-2016-2017 Spreading Excellence and Widening Participation under grant agreement No 809965.

Author(s)	Valentina Janev (PUPIN), Christoph Lange (Fraunhofer)
Contributor(s)	
Internal Reviewer(s)	Christoph Lange (Fraunhofer)
Approval Date	
Remarks	

Workpackage	WP 1 Project Management
Responsible for WP	Institute Mihajlo Pupin
Deliverable Lead	Institute Mihajlo Pupin (Valentina Janev)
Related Tasks	Task 1.3 Quality control, risk management and self-assessment

Document History and Contributions

Version	Date	Author(s)	Description
0.1	1.10.2018	Valentina Janev	First draft
0.2	19.12.2018	Christoph Lange	Contribution and Review
0.3			
0.4			

Executive Summary

This document entitled “Data Management Plan” (DMP) outlines the strategy for data management to be applied throughout the course of the LAMBDA project, as well as the actions that will be taken after the LAMBDA project has been finished. It is based on the “Guidelines on Data Management in Horizon 2020” document and follows the FAIR Data management principles. The DMP will be updated in the course of the project whenever significant changes arise, in addition to the periodic evaluation/assessment of the project.

Table of Contents

Abbreviations and Acronyms

DoA	Description of the Action
DMP	Data Management Plan
FAIR	Findable, Accessible, Interoperable and Reusable
OERs	Open Educational Resources

List of Tables

1. Introduction

The main focus of the LAMBDA (**L**earning, **A**pplying, **M**ultiplying **B**ig **D**ata **A**nalytics)[1] project data management framework is to ensure that the project's generated and gathered data can be preserved, exploited, shared or reuse in a consistent manner. Following the EC requirements and FAIR Data Management Principles, LAMBDA has established infrastructure for managing the Research Data and other project outputs effectively, while the metadata attached to them will make them discoverable, accessible, assessable, usable beyond the original purpose and exchangeable between researchers. Partners [2] involved in the LAMBDA project and their roles in data management are given in Table 1. All partners contribute to LAMBDA outputs according to the LAMBDA Work Plan described in the Description of the Action (DoA).

Table 1. LAMBDA partners and main data management roles

Short name	Partner	Organization Type	Main data management role
PUPIN	Institute Mihajlo Pupin, Serbia (Coordinator)	Research and Development Institute	- Maintain the LAMBDA platform and data used for experimentation
IAIS	Fraunhofer Institute for Intelligent Analysis and Information Systems, Germany	Research and Development Institute	- Support PUPIN team in experimentation with open-source tools and development of proof-of-concept solutions
UBO	Institute for Computer Science - University of Bonn, Germany	University	- Provide learning material as Open Education Resources (OERs) via SlideWiki.org
UOXF	Department of Computer Science - University of Oxford, UK	University	- Provide learning material as Open Education Resources (OERs) via SlideWiki.org

1.1 Scope

A Data Management Plan (DMP) is a structured guideline that describes the comprehensive lifecycle of research data, from conception to storage, analysis, and preservation. DMPs help researchers to think through all relevant questions concerning the data their research will generate, and ensure attention remains focused on the long-term accessibility and subsequent reusability of their data assets. The definition of Research data is defined in the "Guidelines on Open Access to Scientific Publication and Research Data in Horizon 2020" (2015) as:

> "Research data refers to information, in particular facts or numbers, collected to be examined and considered and as a basis for reasoning, discussion, or calculation. In a research context, examples of data include statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings and images. The focus is on research data that is available in digital form."

[1] http://www.project-lambda.org/
[2] https://project-lambda.org/Partners

According to the EC provided documentation[3] for data management in H2020, aspects like research data access, sharing and security should also be addressed in the DMP. This document has been produced following these guidelines and aims to provide a policy for the project partners to follow.

1.2 Relation to Other Deliverables

This Deliverable is related to

1. Deliverable 1.2 External and intra-consortium e-collaboration tool v1, which describes the LAMBDA platform and services for information sharing, easier and more effective collaboration among consortium members, as well as management of the stakeholders database.
2. Deliverable 3.1 The 'Trainers' Network' Infrastructure, which describes the private part of the LAMBDA platform, the link to the SlideWiki.org server and Knowledge repository for storing lectures and other learning materials for intra-consortium use only and for sharing with associated partners.
3. Deliverable 5.1 Stakeholders Database and Market Analysis, which describes the private part of the LAMBDA platform and possibilities for storing stakeholders data.

1.3 Structure of the Deliverable

This document contains the main elements of a research data management plan. Section 2 gives an overview of the Data Management Plan. Section 3 describes the data management practice of SlideWiki where the LAMBDA Open Education Resources will be stored. Section 4 describes the data management practice implemented with the LAMBDA platform. Additonally, Section 5 gives examples of Informed Consent Form, 'Terms of Use' and 'Privacy Policy' documents. Section 6 points to the FAIR principles that will be followed in the LAMBDA project.

[3] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

2. LAMBDA DMP in a Nutshell

The Data Management Plan addresses all the data sets that will be collected, processed and/or generated within the project. Five types of datasets will be produced and/or collected during the LAMBDA project, as is presented in Table 2.

Table 2. Main LAMBDA datasets

	Dataset	Open / Restricted	Sharing medium	Preservation Duration	Costs
(1)	**Learning materials**	Open	SlideWiki.org server	5 years	no extra cost
(2)	**Datasets for experimentation**	Restricted	LAMBDA-Project.org	5 years	no extra cost
(3)	**Stakeholders data**	Restricted	LAMBDA-Project.org	5 years, If appropriate consent is given	no extra cost
(4)	**Proof-of-concept applications**	Restricted	LAMBDA-Project.org	5 years	no extra cost
(5)	**Open source tools, Research papers, Analyses, Case studies**	Open	LAMBDA-Project.org	5 years	no extra cost

Being in line with the EU's guidelines regarding the DMP (European Commission, 2016), this document should address for each data set collected, processed and/or generated in the project the following elements:

1. Data set reference and name - In order to be able to distinguish and easily identify data sets, each data set is assigned with a unique name.
2. Data set description - Each data set that will be collected, processed or generated within the project will be accompanied by a brief description.
3. Standards and metadata
4. Data sharing
5. Archiving and preservation

Table 2 provides a basic description of the data sets with details about what will happen to the data both during the project and after it has been completed. Data set naming rules will be defined in the WP3 and WP4 framework in course of the project.

Table 3. LAMBDA DMP Version 1.0

Data Collection and Documentation	
How are the data generated and which data are re-used?	(1) The consortium aims to generate **high quality online learning materials**, also known as Open Educational Resources (OERs). OERs can be described as teaching, learning and research resources that reside in the public domain or have been released

	under an intellectual property license that permits their free use or repurposing by others depending on which Creative Commons license is used[4]. (2) Additionally **proprietary data will be re-used for experimentation** with Big Data Analytics tools. These datasets will be restricted to the consortium only. (3) Stakeholders data will be collected based on a given consent during registration and based on their involvement in LAMBDA events. (4) Development of solutions for associated partners that have signed a non-disclosure agreement (5) Research papers and other documents ready for dissemination
How will the data be documented?	LAMBDA researchers will follow best practices for documenting the results.
What metadata are needed to sufficiently describe and thus understand the data?	Metadata should include the following overall features of **learning materials**: The title and a description; the keywords describing the material; the date of publication; the entity responsible (publisher) for making the material available; the contact point of the material; the themes/categories covered by the material. Within the context of the semantic representation of SlideWiki, existing ontologies and vocabularies for semantic representation of OpenCourseWare material and enhancement of these for capturing SlideWiki representations will be reviewed and the resulting vocabulary will support representation of content, structure, metadata, provenance and revision history.
Ethics, legal and security issues	
Are the data subject to personal rights or copyrights?	(1) and (5) Open data subject to licenses such as the Creative Commons Attribution 4.0 License (CC-BY) [5] is preferred. The **Creative Commons Attribution 4.0** License will allow the learning material to be shared and adapted for any purpose, even commercially. The only restriction is attribution: linking to the source and indicating the changes made. Released in November 2013, CC-BY 4.0 improves over its predecessor CC-BY 3.0, as it is an international license and includes databases. The created content itself will be published in an open manner without usage restrictions or license costs. However the content itself shall keep records with regard to authorship, modifications and possibly also its usage. Links and credits to original data sources should be given. This is particularly important for scientific publications. (2) (3) and (4) With regard to experimentation with Big Data Analytics tools, where possible, the project will make use of **existing open source libraries** and make its efforts highly visible and open to external input, aiming thus to attract collaboration rather than competition.
Are there other legal contracts that have to be respected?	The Consortium Agreement defines the Access Rights for Exploitation. Parties have identified and agreed on the Background for the Project. The Consortium Agreement also defines the procedure for disclosure of confidential information.

[4] Atkins, D. E., Brown, J. S. & Hammond, A. L. (2007) A Review of the Open Educational Resources (OER) Movement: Achievements, Challenges, and New Opportunities. The William and Flora Hewlett Foundation

[5] https://creativecommons.org/licenses/by/4.0/

Do the data have to be modified in a way (e.g. anonymization) that they can be shared?	The consortium members agree to carry out this project in accordance with Data Protection Regulations and will comply with data protection acts, directives, and opinions, both at European and at national level. All beneficiaries will follow local and national regulations regarding data protection and, in the event that the handling of potentially sensitive data becomes a requirement, they will seek to obtain approval from the relevant local/national authority in charge of data protection activities. This is also supported by legal experts in the consortium i.e. the PUPIN Data Protection Officer.
Data Storage and Preservation	
How and where are data stored?	(1) OERs will be stored in the LAMBDA Knowledge repository as well as uploaded to the SlideWiki repository. SlideWiki integrates a Learning Activity Database and the mechanism for logging and collecting all activity data. Prior to registration with SlideWiki, the user should accept the SlideWiki Terms of Use that includes information on Data Protection Policy as well. Based on the consent, SlideWiki seamlessly tracks user actions, associates them with semantically rich events of the activity data model and stores them in the Learning Activity Database. (2) (3) (4) Datasets will be stored in an institutional repository within in the PUPIN premises. LAMBDA consortium members and other stakeholders have access to the data via the project-lambda.org portal.
How often are back ups performed and by whom?	The SlideWiki contents (slides, presentations, questionnaires, diagrams, images, user data etc.) are regularly backed-up and archived by the Fraunhofer IAIS team.
Data sharing and re-use	
How and where are data shared?	(1) Webinars will be organized on monthly basis starting from April 2019. Learning materials will be distributed via the LAMBDA portal and SlideWiki. All datasets in SlideWiki are freely accessible, in particular, under the Open Data Commons Open Database License (ODbL). (2) When access to a dataset is restricted, as is a case with proprietary data, explicit justifications will be given (e.g., ethical, personal data, intellectual property, commercial, privacy-related, security-related).
Who is allowed to access the data?	In order to provide benefit to the European community, most of LAMBDA outputs will be freely accessible. Only the contents stored on the private part of the LAMBDA portal (see also Deliverable 1.2) are restricted to registered users (stakeholders).
How are sensitive data protected?	*Processing and protection of personal data:* The researchers involved in the project will pre-process the data in an anonymous and confidential manner. Collected data will be handled securely, using password protected servers and the enforcing of authorisation mechanisms enabling only privileged staff to have access, as well as the introduction of different levels of access. Personal data in combination with one's personal identity/name will be used exclusively for contacting the stakeholders and for dissemination of information relevant for the LAMBDA project. Detailed information on privacy/confidentiality of any data collected will be provided to the EC and will be clearly explained to all members and participants.

	Deliverables that contain personal data (e.g. D5.1 Stakeholders Database and Market Analysis) will be confidential, restricted under conditions set out in the Grant Agreement.

3. Datasets Available via the SlideWiki Platform

The LAMBDA consortium will develop a series of Big Data Analytics lectures that will be shared with the community via the SlideWiki platform. The strategy for data management in SlideWiki is explained in SlideWiki (GA 688095) Deliverable 12.4 Data Management Plan.[6]

3.1 Implementation of Best Practices in SlideWiki

The SlideWiki platform is a Linked Data platform. Considering the best practices for publishing Linked Data, the following 13 stages are recommended in order to publish a standalone dataset, 6 of them are vital (marked as must).

1. Provide descriptive metadata with locale parameters: Metadata must be provided for both human users and computer applications.
2. Provide structural metadata: Information about the internal structure of a distribution must be described as metadata.
3. Provide data license information: License information is essential to assess data. Data re-use is more likely to happen, if the dataset has a clear open data license.
4. Provide data provenance information: Data provenance describes data origin and history. Provenance becomes particularly important when data is shared between collaborators who might not have direct contact with one another.
5. Provide data quality information: Data quality is commonly defined as “fitness for use” for a specific application or use case.
6. Provide versioning information: Version information makes a dataset uniquely identifiable. The uniqueness enables data consumers to determine how data has changed over time and to identify specifically which version of a dataset they are working with.
7. Use persistent URIs as identifiers: Datasets must be identified by a persistent URI. Adopting a common identification system enables basic data identification and comparison processes by any stakeholder in a reliable way. They are an essential precondition for proper data management and re-use.
8. Use machine-readable standardised data formats: Data must be available in a machine-readable standardised data format that is adequate for its intended or potential use.
9. Data Vocabulary: Standardised terms should be used to provide metadata, Vocabularies should be clearly documented, shared in an open way, and include versioning information. Existing reference vocabularies should be re-used where possible.
10. Data Access: Providing easy access to data on the Web enables both humans and machines to take advantage of the benefits of sharing data using the Web infrastructure. Data should be available for bulk download. APIs for accessing data should follow REST (REpresentational State Transfer) architectural approaches
11. Data Preservation: Data depositors willing to send a data dump for long term preservation must use a well-established serialisation. Preserved datasets should be linked with their "live" counterparts.
12. Feedback: Data publishers should provide a means for consumers to offer feedback.
13. Data Enrichment: Data should be enriched whenever possible, generating richer metadata to represent and describe it.

3.2 Naming Convention of LAMBDA Lectures in SlideWiki

At the time of writing, the contents of the lectures is still under development, however the titles of the lectures will follow a naming convention most often used for open courses, for instance

[6] https://drive.google.com/uc?id=0B52DCt0vMcvab0VrNy1lZy1YR2c&export=download

CODE Lecture #1 (example https://project-lambda.org/EKGs-Lecture-1)

while the CODE is formed based on the Module Title (e.g. Enterprise Knowledge Graphs).

4. Datasets Available via the LAMBDA Platform

LAMBDA consortium has established a Knowledge repository[7] as part of the LAMBDA Platform that will facilitate spreading excellence and exchange of learning materials and best practice between the international leading organizations and stakeholders (research institutions and industry) from the West Balkan countries. The repository is part of the private part of the LAMBDA portal where the access is restricted to registered users.

4.1 Naming Convention of LAMBDA materials

At the time of writing, the Knowledge repository is still empty. The following URIs have been introduced for different entries to the knowledge repository:

https://project-lambda.org/Knowledge-repository/Lectures
https://project-lambda.org/Knowledge-repository/Datasets
https://project-lambda.org/Knowledge-repository/Tools
https://project-lambda.org/Knowledge-repository/Projects

Additionally datasets will follow the naming convention as is presented in Table 4.

Table 4. Naming convention for LAMBDA datasets used for experimentation

Title	Open / Restricted	Data standard	Metadata standard
Domain.Stakeholder.Dataset_1	TBD	CSV, JSON, RDF	TBD
Domain.Stakeholder.Dataset_2			
Domain.Stakeholder.Dataset_3			

In the following sections, we explain what types of data we record when a user visits the LAMBDA portal, and precisely how they are used:

4.2 Recording and Processing of Data in Connection with Access over the Internet

When a user visits the LAMBDA platform, our Web server makes a temporary record of each access and stores it in a log file. The following data are recorded, and stored until an automatic deletion date:

1. IP address of the requesting processor
2. Date and time of access
3. Name and URL of the downloaded file
4. Volume of data transmitted
5. Indication whether the download was successful
6. Web site from which our site was accessed

[7] https://project-lambda.org/Knowledge-reporitory

The purpose of recording these data is to allow use of the Web site (connection setup), for system security, for technical administration of the network infrastructure and in order to optimize our Internet service. The IP address is only evaluated in the event of fraudulent access to the network infrastructure of PUPIN.

Apart from the special cases cited above, the consortium do not process personal data without first obtaining an explicit consent to do so.

4.3 Use and Transfer of Personal Data

The consortium will use the information held about the users in the following ways:

- to carry out our obligations arising from the LAMBDA project;
- to provide users/visitors with information about the LAMBDA project;
- to allow users/visitors to participate in interactive features of LAMBDA services; to provide users/visitors, or permit other registered users to receive information as a result of subscription to the LAMBDA content and/or match-making functionalities of the LAMBDA platform.

All use of users/visitors personal data is confined to the purposes stated above, and is only undertaken to the extent necessary for these purposes. The users/visitors data is not disclosed to third parties. Personal data will not be transferred to government bodies or public authorities except in order to comply with mandatory national legislation or if the transfer of such data should be necessary in order to take legal action in cases of fraudulent access to our network infrastructure. Personal data will not be transferred for any other purpose.

4.4 Security

The PUPIN Institute implements technical and organizational security measures to safeguard stored personal data against inadvertent or deliberate manipulation, loss or destruction and against access by unauthorized persons. Our security measures are continuously improved in line with technological progress.

4.5 Links to Web sites Operated by Other Providers

The LAMBDA platform may contain links to other providers' Web pages. We would like to point out that this statement of data protection conditions applies exclusively to the Web pages managed by PUPIN. We have no way of influencing the practices of other providers with respect to data protection, nor do we carry out any checks to ensure that they conform with the relevant legislation.

4.6 Right to Information and Contact Data

At any time, registered users have the right to request from the administrator: the access to their personal data, change, deletion or restriction of data processing and data transfer rights, or to file an objection to data processing. Users also have the right to withdraw their consent and the right to receive a copy of their personal data that are being processed. Users can accomplish all of these rights by sending a request to the data administrator via email address: dejan.paunovic@pupin.rs.
The users have the right to ask us not to process their personal data for marketing purposes. The LAMBDA server will usually inform the user (before collecting his/her data) if we intend to use your data for such purposes. Users have the possibility to manage his/her profile and delete his/her profile at any time.

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If the user follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

In the case of unauthorized data processing, the users have all rights from the General Data Protection Regulation, GDPR, (EU citizens) and Law on personal data protection (citizens of the Republic of Serbia), whose application is supervised by the Commissioner for information of public importance and personal data protection (via email: **office@poverenik.rs**).

For mote information, please check Section 5.3 Privacy Policy.

4.7 Sustainability

PUPIN will maintain and update the LAMBDA portal and sustaining project activities for at least five years (5) after the end of the project as part of the PUPIN TTO activities.

5. Data Protection Issues

The consortium members agree to carry out this project in accordance with Data Protection Regulations and will comply with data protection acts, directives, and opinions, both at European and at national level, including:

- the General Data Protection Regulation 2016/679;
- the Charter of Fundamental Rights of the EU, specifically the article concerning the protection of personal data;
- and the opinions of the European Group on Ethics in Science and New Technologies in their report “Citizens Rights and New Technologies: A European Challenge” on the Charter on Fundamental Rights related to technological innovation.

During the course of this project, consortium members will take all the necessary steps to ensure that all participants understand the objectives of this project and the processes employed during LAMBDA to achieve them. All beneficiaries will follow local and national regulations regarding data protection and, in the event that the handling of potentially sensitive data becomes a requirement, they will seek to obtain approval from the relevant local/national authority in charge of data protection.

5.1 Processing and Protection of Personal Data

The researchers involved in the project will pre-process the data in an anonymous and confidential manner. Collected data will be handled securely, using password protected servers and the enforcing of authorisation mechanisms enabling only privileged staff to have access, as well as the introduction of different levels of access. Personal data in combination with one's personal identity/name will be used exclusively for contacting the stakeholders and for dissemination of information relevant for the LAMBDA project. Detailed information on privacy/confidentiality of any data collected will be provided to the EC and will be clearly explained to all members and participants. Deliverables that contain personal data (e.g. D5.1 Stakeholders Database and Market Analysis) will be confidential, restricted under conditions set out in the Grant Agreement.

In activities where data/opinion is collected by stakeholders, the involved persons will be informed about the types of questions that the consortium plans to ask, and it will be made clear that people can choose not to answer questions. Participants will be made aware of their ‘withdrawal rights’: that they can withdraw from the interview at any time and that, if they wish, any personal data, recordings or images can be destroyed. An example of an INFORMED CONSENT FORM is given in Table 5. PUPIN will keep on file templates of the informed consent forms and information sheets (in language and terms intelligible to the participants).

Table 5. Informed Consent Form

I, _____
Born on _____/_____/_____ in
Resident in
hereby freely and voluntarily give my CONSENT to participate in the study, organized and conducted by the LAMBDA Consortium.
Giving my consent, I undersign that:
1. I HAVE CAREFULLY READ and UNDERSTOOD THE INFORMATION SHEET.

2. All questions that I posed have been answered to my satisfaction.

3. I AM FULLY AWARE THAT:
- It is my right to withdraw from the study at any time without consequences.
- Any videos, pictures, audio recordings, and information about myself will be treated as confidential by the research team members.
- Videos, pictures and audio recordings will be stored in a protected folder by the research team and

only used for research purposes related to the evaluation of the LAMBDA project.
- In any publication resulting from the LAMBDA project, my personal details will not be revealed and it will not be possible to retrieve any data which might disclose my identity;
- My address and other personal identifiable information may be disclosed upon my consent only in case of formal ethical investigations by scientific journals or academic societies challenging the existence itself of this empirical investigation.

Strike out whichever does not apply:

HAVING READ, UNDERSTOOD AND ACCEPTED ALL OF THE ABOVE,
 I agree/do not agree to participate in the interview;

 I agree/do not agree to any session being audio taped and video recorded;

 I agree/do not agree that short extracts of video or photograph recordings, in which what I say or what I do cannot be precisely determined and that cannot in any way damage my reputation, may be used by the LAMBDA Consortium members for dissemination and illustrative purposes of the research results;

 I would like/would not like to receive publications stemming from the direct analysis of this experimental activity.

For the sole purpose of receiving these publications I provide here my email address _____

Place _____ Date: _____/_____/_____

Signature of the Participant: _____

For the need of the project, as part of the LAMBDA platform[8], two public pages have been created. At registration, the LAMBDA user has to give consent to

- the Terms of Use
- the LAMBDA Privacy Policy

5.2 Example: Terms of Use

The **Terms of Use** document was defined by the PUPIN Legal Department and controlled by other LAMBDA partners from Germany (IAIS and UBO) and UK (UOXF). The text of the document is included in this documentation.

This is a human-readable **summary** of the Terms of Use for LAMBDA Platform.

Disclaimer: This summary is not a legal document. It is simply a handy reference for understanding the 'Terms of Use'. Think of it as the user-friendly interface to the legal language of LAMBDA 'Terms of Use'. By registering with the LAMBDA platform you will give consent for your data to be stored in LAMBDA database and processed for the purposes of the LAMBDA project. Please, visit also the Privacy Policy page.

Registered users are free to:

- **Create** a profile of their company and **Use** the possibilities of the **LAMBDA Tools** for networking.
- Re-use the **LAMBDA Learning materials**.

Under the following conditions

- **Responsibility** – You take responsibility for your edits (since we only *host* your content).

[8] https://project-lambda.org/

- **Civility** – You support a civil environment and do not harass other users.
- **Lawful behaviour** – You do not violate copyright or other laws.
- **No Harm** – You do not harm our technology infrastructure.
- **Terms of Use and Policies** – You adhere to the Terms of Use and to the applicable community policies when you visit our sites or participate in our communities.

With the understanding that

- This service may contain **translations** powered by third party services. Selecting to use the translate service will result in data being sent to third-party services. We disclaims all warranties related to the translations, expressed or implied, including any warranties of accuracy, reliability, and any implied warranties of merchantability, fitness for a particular purpose and noninfringement.
- **You license freely your contributions;** the contents (images) you upload will be is in the public domain.

Refraining from Certain Activities

We reserve the rights to remove content that we consider to be inappropriate, offensive or spam. Certain activities, whether legal or illegal, may be harmful to other users and violate our rules, and some activities may also subject you to liability. Therefore, for your own protection and for that of other users, you may not engage in such activities on our sites.

These activities include:

Harassing and Abusing Others

- Engaging in harassment, threats, stalking, spamming, or vandalism; and
- Transmitting chain mail, junk mail, or spam to other users.

Violating the Privacy of Others

- Infringing the privacy rights of others under the EU General Data Protection Regulation (GDPR) or other applicable laws (which may include the laws where you live or where you view or edit content); The EU GDPR Regulation aims to strengthen the rights of individuals to manage personal data held on them.
- Soliciting personally identifiable information for purposes of harassment, exploitation, violation of privacy, or any promotional or commercial purpose not explicitly approved by the project; and
- Soliciting personally identifiable information from anyone under the age of 18 for an illegal purpose or violating any applicable law regarding the health or well-being of minors.

Engaging in False Statements, Impersonation, or Fraud

- Intentionally or knowingly posting content that constitutes libel or defamation;
- With the intent to deceive, posting content that is false or inaccurate;
- Attempting to impersonate another user or individual, misrepresenting your affiliation with any individual or entity, or using the username of another user with the intent to deceive; and
- Engaging in fraud.

Committing Infringement

- Infringing copyrights, trademarks, patents, or other proprietary rights under applicable law.

Misusing Our Services for Other Illegal Purposes

- Posting child pornography or any other content that violates applicable law concerning child

pornography;
- Posting or trafficking in obscene material that is unlawful under applicable law; and
- Using the services in a manner that is inconsistent with applicable law.

Engaging in Disruptive and Illegal Misuse of Facilities

- Posting or distributing content that contains any viruses, malware, worms, Trojan horses, malicious code, or other device that could harm our technical infrastructure or system or that of our users;
- Engaging in automated uses of the site that are abusive or disruptive of the services and have not been approved by the project community;
- Disrupting the services by placing an undue burden on a project website or the networks or servers connected with a project website;
- Disrupting the services by inundating any of the project websites with communications or other traffic that suggests no serious intent to use the project website for its stated purpose;
- Knowingly accessing, tampering with, or using any of our non-public areas in our computer systems without authorization; and
- Probing, scanning, or testing the vulnerability of any of our technical systems or networks unless all the following conditions are met:
    - such actions do not unduly abuse or disrupt our technical systems or networks;
    - such actions are not for personal gain (except for credit for your work);
    - you report any vulnerabilities to project's developers (or fix it yourself); and
    - you do not undertake such actions with malicious or destructive intent.

5.3 Example: Privacy Policy

This Policy (together with our Terms Of Use and any other documents referred to on it) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

Information We May Collect From You

We may collect and process **Information/Contents you give us** or you upload to the platform. You may give us information about you by filling in forms on our site. This includes information you provide when you register to use our site, subscribe to our service, or participate in Ideas & Discussions section on the private part of the portal. The information you give us may include your name, e-mail address, images of the material to be promoted via the LAMBDA Network. Your personal data and all contents uploaded by you will be stored in the LAMBDA database maintained by the Institute Mihajlo Pupin.

Uses Made of The Information

We use information held about you in the following ways:

- to carry out our obligations arising from the LAMBDA project;
- to provide you with information about the LAMBDA project;
- to allow you to participate in interactive features of our service, when you choose to do so; to provide you, or permit other registered users to receive information as a result of subscription to the LAMBDA content and/or match-making functionalities of the LAMBDA platform.

Your Rights

At any time, you have the right to request from the administrator: the access to your personal data, change, deletion or restriction of data processing and data transfer rights, or to file an objection to data processing. You also have the right to withdraw your consent and the right to receive a copy of your personal data that

are being processed. You can accomplish all of these rights by sending a request to the data administrator via email address: dejan.paunovic@pupin.rs.

You have the right to ask us not to process your personal data for marketing purposes. We will usually inform you (before collecting your data) if we intend to use your data for such purposes. You have the possibility to manage your User profile and delete your profile at any time.

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

In the case of unauthorized data processing, you have all rights from the General Data Protection Regulation, GDPR, (EU citizens) and the Law on personal data protection (citizens of the Republic of Serbia), whose application is supervised by the Commissioner for information of public importance and personal data protection (via email: **office@poverenik.rs**).

Changes to our Privacy Policy

Any changes we may make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes to our privacy policy.

Contact

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to info@pupin.rs

6. FAIR Data Management Principles

The FAIR principles are a set of community-developed guidelines to ensure that data or any digital object are Findable, Accessible, Interoperable and Reusable. The FAIR principles specifically emphasize enhancing the ability of machines to automatically find and use data or any digital object, and support its reuse by individuals. Standards for the description, interoperability, citation etc. are at the core of these principles. The LAMBDA consortium monitors the application of the FAIR Data management principles, also listed here below.

6.1 Making Data Findable, Including Provisions for Metadata

- Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?
- What naming conventions do you follow?
- Will search keywords be provided that optimize possibilities for re-use?
- Do you provide clear version numbers?
- What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

6.2 Making Data Openly Accessible

- Which data produced and/or used in the project will be made openly available as the default? If certain datasets cannot be shared (or need to be shared under restrictions), explain why, clearly separating legal and contractual reasons from voluntary restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if relevant provisions are made in the consortium agreement and are in line with the reasons for opting out.
- How will the data be made accessible (e.g. by deposition in a repository)?
- What methods or software tools are needed to access the data?
- Is documentation about the software needed to access the data included?
- Is it possible to include the relevant software (e.g. in open source code)?
- Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories, which support open access where possible.
- Have you explored appropriate arrangements with the identified repository?
- If there are restrictions on use, how will access be provided?
- Is there a need for a data access committee?
- Are there well described conditions for access (i.e. a machine readable license)?
- How will the identity of the person accessing the data be ascertained?

6.3 Making Data Interoperable

- Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?
- What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?
- Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability?

- In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?

6.4 Increase Data Re-use (through clarifying licences)

- How will the data be licensed to permit the widest re-use possible?
- When will the data be made available for re-use? If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.
- Are the data produced and/or used in the project useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why.
- How long is it intended that the data remains re-usable?
- Are data quality assurance processes described?

6.5 Allocation of Resources

- What are the costs for making data FAIR in your project?
- How will these be covered? Note that costs related to open access to research data are eligible as part of the Horizon 2020 grant (if compliant with the Grant Agreement conditions).
- Who will be responsible for data management in your project?
- Are the resources for long term preservation discussed (costs and potential value, who decides and how what data will be kept and for how long)?

6.6 Data Security

- What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?
- Is the data safely stored in certified repositories for long term preservation and curation?

6.7 Ethical Aspects

- Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and the ethics chapter in the Description of the Action (DoA).
- Is informed consent for data sharing and long term preservation included in questionnaires dealing with personal data?

6.8 Other issues

- Do you make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones?

7. Conclusion

This deliverable outlines the guidelines and strategies for data management within the context of the LAMBDA project and will be fine-tuned and extended throughout the course of the project. Following the guidelines on FAIR Data Management in H2020[9] and Data Management in H2020[10], we described the purpose and scope of learning materials that will be stored in the SlideWiki repository, and other datasets' management as part of the private side of the LAMBDA portal.

[9] European Commission, [Online]. Available: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[10] European Commission, [Online]. Available: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.