WP6 Legal and Ethical Requirements

D6.3 – Data Management Plan v.3

The INTERLINK project is co-funded by the European Union.
Horizon 2020 - DT-GOVERNANCE-05-2020 - Grant Agreement No 959201

Project acronym	INTERLINK
Project full title	Innovating goverNment and ciTizen co-dEliveRy for the digitaL sINgle marKet
Call identifier	DT-GOVERNANCE-05-2020
Type of action	RIA
Start date	01/01/2021
End date	31/12/2023
Grant agreement no	959201

WP	WP6, Legal and Ethical Requirements
Author(s)	Diletta De Cicco, Jean De Meyere, Rossana Ducato, Quentin Fontaine, Charles-Albert Helleputte, Alain Strowel, Aurore Troussel (UCL)
Editor(s)	N/A
Reviewers	Anna Benedetti (Ethics Advisory Board), Danilo Giampiccolo (FBK), Luc Desaunettes-Barbero (UCL)
Leading Partner	UCL
Version	V1.0
Deliverable Type	ORDP
Dissemination Level	PU
Date of Delivery	31/12/2023
Submission Date	30/12/2023

VERSION HISTORY

Version	Issue Date	Status	Changes	Contributors
V 0.1 - DRAFT	24.11.2023	Draft		UCL
V 0.2 – DRAFT	13.12.2023	Prefinal	Integration of contribution by project partners and reviewers	All Partners + EAB
V 1.0	31.12.2023	Final	Integration of comments based on the final review	UCL – FBK

Table of contents

Executive summary

This deliverable describes the data management life cycle for all data sets that are collected, processed or generated by the project. A Data Management Plan is a document specifying how research data will be handled both during and after a research project. It identifies key actions and strategies to ensure that research data are of a high-quality, secure, sustainable, and – to the extent possible – accessible and reusable.

The European Commission is running a flexible pilot under Horizon 2020 called the Open Research Data Pilot (ORD pilot). A Data Management Plan is required for all projects participating in the extended ORD pilot in Horizon 2020, unless they opt out of the ORD pilot. However, projects that opt out are still encouraged to submit a DMP on a voluntary basis.

INTERLINK used the Horizon 2020 FAIR DMP template provided in DMPonline. be that is based on the Horizon 2020 FAIR DMP template developed by the European Commission, the use of which is recommended but voluntary. The Commission's template has been designed to be applicable to any Horizon 2020 project that produces, collects or processes research data. It is inspired by the concept of FAIR data, i.e. research data that are findable, accessible, interoperable and re-usable.

1 Data summary

1.1 What is the purpose of the data collection/generation and its relation to the objectives of the project?

The aim of INTERLINK is to overcome the barriers that prevent public administrations from efficiently sharing services in a Digital Single Market by combining the enthusiasm and flexibility of grassroots initiatives with the legitimacy and accountability granted by top-down e-government frameworks. INTERLINK 's hypothesis is that by implementing a public-citizen partnership that combines the bottom-up approach of citizens' initiatives with the top-down approach of traditional e-government frameworks, we can lower the barriers that public administrations encounter to efficiently reuse, share, and deliver services collaboratively.

INTERLINK pursues 5 main objectives. Each of them requires the collection and/or generation of data:

1. To develop a new collaborative governance model based on partnerships between public administrations, citizens and companies. To achieve this goal, INTERLINK has collected data from public administrations, citizens and non-governmental organizations to assess their needs in terms of governance models and analyze current and/or planned partnerships.

2. To provide a set of Interlinkers (i.e., digital enablers that will standardize the basic functionalities needed by private actors to co-produce a service), in order to remove technological barriers and promote the delivery of interoperable, inclusive, sustainable and ethical public services. To achieve this goal, INTERLINK has collected data from private actors in relation to public services.

3. To deliver the INTERLINK framework and operational platform, that rely on an open software system leveraging on mobile communication to facilitate the co-production of services between public administrations and private stakeholders. To achieve this goal, INTERLINK haa collected data from public administrations and private stakeholders to identify their needs in terms of co-production of services. The data collection allows INTERLINK to understand what is already in place and what can be created. The data generated is related to service providers and services.

4. To identify the legal framework for co-creation and co-delivery of services, to ensure that the INTERLINK enablers and governance models comply with EU laws and are usable for cross-border services. To achieve this goal, INTERLINK has collected data on the regulation of activities carried out by INTERLINK and its stakeholders (including use case members).

5. To evaluate and assess the impact of the INTERLINK solution in three proof-of-concept use cases that represent meaningful and complementary examples of the class of services targeted by INTERLINK. To achieve this objective, INTERLINK has collected data from citizens, companies, public administrations and other stakeholders of each use case. These data have been analyzed to assess citizen participation and understand the social impact of the project.

In order to make the project objectives measurable and validate the project approach, use cases have been developed and implemented within each of the three public administrations of the consortium: the Italian Ministry of Economy and Finance (MEF), the Latvian Ministry of Environmental Protection and Regional Development (VARAM) ,and the City of Zaragoza (ZGZ).

In general, INTERLINK 's data collection pursues the above objectives and purposes. Since INTERLINK aims to connect public administrations, citizens and non-governmental organizations, these three groups have been analyzed through data collection and processing. In addition, INTERLINK has collected data related to the production and provision of services, as our objective is to provide a platform that enables these services.

INTERLINK communicates about its activities. In particular, INTERLINK has its own website and communicates the project's outcomes through press releases, newsletters, social media and events. INTERLINK also relies on social media platform LinkedIn to share news on the advancement of the project. The data processing related to these activities serves the general purpose of communicating about INTERLINK.

Personal data have beencollected to evaluate and assess the impact of the INTERLINK solution, to verify user's participation in the INTERLINK project and for marketing and communication purposes. Personal data collection has been carried out in respect with the current EU legislation, notably the General Data Protection Regulation (GDPR)[1].

1.2 What types and formats of data will the project generate/collect?

In this DMP, the data collected by INTERLINK are classified into five categories: internal management data (1), research data (2), communication data (3), use case data (4) and Interlinkers. Answers below are broken down among those categories.

1. Internal management data : i.e., all data necessary to manage to correct course of the project. They are exchanged between individual consortium members or representatives of partner institutions to manage and coordinate the project. This data collection is managed and supervised by FBK as theproject coordinator (WP1).

2. **Research data** : i.e., all recorded factual material generally accepted in the scientific community as necessary to validate research findings.

The data collected and generated is textual and numerical in nature (including statistics).

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ L*, 119, 27 avril 2016.

The data objects collected and generated are text documents, spreadsheets, questionnaires, videotapes, and audio recordings.

The data was collected through different modes including documents (e.g., reports, laws and ordinances, meeting minutes), interviews, surveys, focus groups, observations, compilations, websites (e.g., from other European cases of collaborative platforms), extraction from open databases and from the INTERLINK partners' database (e.g., FBK will reuse data from other European projects, MEF will reuse previously collected data, etc.).

3. Communication data : i.e., all data produced to create communication content and data necessary to disseminate communication relevant to INTERLINK.

This data includes images (jpeg; png) and documentation (.xls; .doc; .pdf) that have been collected from partners and stored in a secure Google Drive to update the website. The communication team (WP7) has used these data for the moment only for the project website and the social network LinkedIn.

4. Use case data :i.e., data related to the three uses cases implemented in Spain (ZGZ), Latvia (VARAM) and Italy (MEF). Use casa data have included personal data.

INTERLINK hascollected and processed personal data of the participants to each use case. The following personal personal data have been collected for the purposes of evaluating and assessing the impact of the INTERLINK solution and to verify user's participation in the INTERLINK project:

- Name
- Address
- Email
- Phone number
- Age
- Gender
- Picture
- Education level
- Professional field and status
- Activity while using the Interlinkers (e.g. logs)

5. Interlinkers: i.e., digital enablers that standardizes the basic functionalities needed by private actors to co-produce a service. Interlinkers are divided between software Interlinkers and knowledge Interlinkers (e.g. technical or procedural documentation/templates/etc...).

Some Interlinkers are external and have been provided by external actors. Some Interlinkers are internal and were directly developed by project partners.

Formats of data:

INTERLINK uses data formats that ensure access, reuse and future storage of the data. INTERLINK primarily uses digital data formats such as:

- for text data, Rich Text Format (.rtf), plain text, ASCII (.txt), eXtensible Mark-up Language (.xml), Hypertext Mark -up Language (.html) and widely used formats: MS Word (.doc/.docx);
- for image data: TIFF 6.0 uncompressed (.tif), JPEG (.jpeg, .jpg, .jp2) if the original was created in this format, GIF (.gif) PNG (.png) Adobe Portable Document Format (PDF/A, PDF) (.pdf);
- for audio data, Free Lossless Audio Codec (FLAC) (.flac), MPEG-1 Audio Layer 3 (.mp3) if the original was created in this format, and Waveform Audio Format (.wav);
- for video, MPEG-4 (.mp4);
- for documentation and scripts, Rich Text Format (.rtf) , PDF/UA, PDF/A or PDF (.pdf), XHTML or HTML (.xhtml, .htm), OpenDocument Text (.odt), plain text (.txt) widely used formats: MS Word (.doc/.docx), MS Excel (.xls/.xlsx).

These file formats were chosen because they are accepted standards and are widely used. For long-term storage, files have beenconverted to open file formats when possible.

1.3 Will you re-use any existing data and, if so, how?

INTERLINK hasreused data only when permitted to do so, in compliance with applicable regulatory or contractual restrictions (e.g., confidentiality agreements, etc.). INTERLINK has relie on the Data Processing Agreement present in Annex 4 when sharing personal data with each other. INTERLINK has not shared personal data with third parties unless the necessary agreements are in place. Personal data may have shared between INTERLINK partners through the use of appropriate Personal Data Agreements.

In this DMP, the data collected by INTERLINK are classified into five categories: internal management data (1), research data (2), communication data (3), use case data (4) and (5) Interlinkers. Answers below are broken down among those categories.

1. Internal management data : INTERLINK has drawn on other projects to reuse and improve work already done. This includes, for example, results from previous EU or nationally funded projects and other types of initiatives that can be applied to INTERLINK's objectives. the methodology used in two previous projects, namely Digital Hub and WeLive Co-creation Methodology, is an inspiration for INTERLINK partners.

2. **Research data** : INTERLINK has used data collected by other academics and researchers, as well as members of the project.

3. Communication data : N/A

4. Use case data : INTERLINK has reused data processed by the Italian Ministry of Economy and Finance (MEF), the Latvian Ministry of Regional Development (VARAM) and the City of Zaragoza (ZGZ). This was necessary to achieve INTERLINK's objectives in relation to the specific use case.

5. Interlinkers: External Interlinkers were established through data reused from various external sources.

1.4 What is the origin of the data?

In this DMP, the data collected by INTERLINK are classified into five categories: internal management data (1), research data (2), communication data (3), use case data (4) and (5) Interlinkers. Answers below are broken down among those categories.

1. Internal management data have been produced by INTERLINK members throughout the course of the project. Data exchange has been performed by e-mail, Google Drive, using various common software tools (Miro boards, Microsoft Excel spreadsheets, Microsoft Word documents, etc.).

2. Research data has been collected for a literature review as parts of the research on governance models of Radboud University (WP2). Electronic databases (Web of Science, GoogleScholar) was used to find open access publications. Records were manually screened for title and abstract and by reading the full text when required. Second, data is collected accessed through RuQuest. Third, experts known in the field of co-production were asked to add further texts to the literature list. The references to this research were stored on EndNote and coded in Atlas.ti.

Subsequently, WP2 also has collected focus group- and interview data from the use cases, for both the explorative part of the use-case analysis (leading to the preliminary governance model) and the case study research as basis for the advanced governance model. Furthermore, data (documents and interviews) was collected for eight cases of digital collaborative platforms covering eleven countries as well as all levels of government with a predominance of the local one. The empirical investigation was based on 1) the collection of documents, 2) focus groups and 3) semi-structured interviews. Documents included relevant digitalisation policies and strategies, organisational charts, action plans as well as reports. In contrast, focus groups and semi-structured interviews were rather focused on the lived experiences of stakeholders.

Two focus groups were conducted with representatives of the INTERLINK pilots. Subsequently, we conducted 15 interviews among all cases. The respondents that were present during the focus groups (MEF, VARAM and ZGZ) signed the INTERLINK 'informed consent' documents and thus agreed to be recorded for both focus group sessions and subsequent interviews.

Interview respondents included public officials at both the managerial and working level of the public organisations under investigation as well as external experts on the respective platforms and the process of their development. All respondents agreed to an online interview. Consent was given in the beginning of each interview regarding both a recording and the use of transcribetranscripts. The audio-files are stored on Surfdrive, as well as the transcriptions. They are coded in Atlas.ti. Direct and indirect anonymised quotes are used in the reports and academic publications. Finally, several cases in

Europe were identified and further investigated, through desk research and interviews. The respondents all signed the 'informed consent' document and thereby also agreed to the online interviews being recorded. The audio-files and the transcriptions are stored in Surfdrive and coded in Atlas.ti.

UCL (WP6) has relied on a similar approach to produce the report on legal requirements for the project. The EUR-Lex database has been used to research and obtain relevant EU legal texts (notably the GDPR, the Data Act, the Data Governance Act and the Digital Services Act).

3. Communication data, Data have beencollected via emails from the different partners and stored via Google Workplace Tools, like Drive, which is managed by FBK as project manager (WP1).

4. Use case data: In the context of the deployment of the use cases, MEF, VARAM and the city of Zaragoza (Spain) collected data from those use cases. The Interlinkers developed within the consortium will contribute to the data collection.

MEF (Italy) collected quantitative and qualitative data to test the usability of the Participatory Strategic Planning Module ("PSPM"). During the co-design phase of the PSPM, MEF collected data from other public administrations through meetings, questionnaires and surveys. During the preparation and implementation phases of the PSPM, data were collected from other public/private associations, public administrations and citizens through questionnaires and surveys. MEF also surveyed its own staff and collect data.

VARAM (Latvia) collected data on the operation of Customer Service Centers, in Word and Excel formats. The necessary information were provided by Customer Service Centers themselves. Statistical data on public services were provided by the owners of the services (institutions, municipalities), and statistical data on the use of service descriptions in the State Service Portal were collected by the State Agency for Regional Development (subordinate institution of VARAM). These datasets will remain available as open datasets on the Latvian Open Data Portal, collected through the use of Google Analytics.

The City of Zaragoza (Spain) collected different types of data: quantitative, qualitative, survey data, experimental measurements, images, audiovisual data, etc. They will be collected from the advertising program "Volveremos Si Tú Vuelves", Zaragoza City Card, user data from Etopia Center for Arts and Technology. The data were retrieved from databases using API and FTP access or, in the case of Etopia, through the standard web interface of Eventbrite.

5. Interlinkers : external Interlinkers were directly obtained from external sources, while internal Interlinkers were directly produced by members of the Consortium. For more information, the complete list of Interlinkers can be consulted on the INTERLINK demo platform.

1.4 What is the expected size of the data (if known)?

The size of the data collected throughout the project does exceed several TB and therefore does not require significant storage capacity. There are be minimal costs associated with managing storage and no particular challenges associated with transferring data.

The expected size of the data for internal management is expected to be on the order of megabytes, as is the INTERLINK research data.

The size of the data for the use cases will depend on the type of Interlinkers used and the use cases. It is estimated to be on the order of several GB (e.g., 50 GB estimated by VARAM).

1.5 To whom might the data be useful ('data utility')?

In this DMP, the data collected by INTERLINK are classified into four categories: internal management data (1), research data (2), communication data (3), and use case data (4). Answers below are broken down among those categories.

1. Internal management data are not useful to third parties.

2. **Research data** could be useful for future research, for public administrations and private companies interested in co-producing digital public services. In addition, INTERLINK research data could be used by academics and researchers for research purposes (e.g., on governance models, digital services, public service platforms, etc.).

3. Communication data could be of interest to other project WPs (e.g., for pilot activities) and to establish the project's exploitation plan.

4. Use case data containing personal data of citizens and organizations participating in INTERLINK and are not reusable. They were used to evaluate Interlinkers and the platform and are not useful to third parties. Reusability of alternative use case data vary per use case :

- Zagaroza: no resuable data.
- VARAM: all data will be kept within consortium except some research and use case data which will be shared with other VARAM departments ONLY in anonymous and aggregated form (as research conclusions) for policy planning needs.
- MEF: The data collected during the co-design phase of the strategic plan, the definition and the implementation of the strategic plan will be accessible to other public administrations and associations only upon direct request to MEF. The data shared on the Open Repository will instead be made available to all (e.g., public administrations, associations, citizens, etc.).

In deciding whether to make data available, INTERLINK considered any applicable regulatory or contractual restrictions (e.g., confidentiality agreements, etc.).

5. Interlinkers are useful for citizens, public and private entities which plan to rely on co-production mechanisms such as those studied in the course of INTERLINK. Their goal is to remove technological barriers and promote the delivery of interoperable, inclusive, sustainable and ethical public services.

2 FAIR data: Making data findable, including provisions for metadata

2.1 Are the data produced and/or used in the project discoverable with metadata?

The consortium followed the principle of "as open as possible, as closed as necessary". It adhered to a policy of open access to all project results, guidelines and reports. Data that were shared rely on metadata for discoverability purposes.

In this DMP, the data collected and/or generated by INTERLINK are classified into four categories: internal management data (1), research data (2), communication data (3), and use case data (4). Answers below are broken down among those categories.

1. Internal management data are not usable by third parties and were not made openly available by default. They rely on the metadata automatically created by Google Drive.

2. Research data generated by the project are made fully reusable, in the form of building blocks where appropriate. They are discoverable through metadata, based on the medium they were published in.

3. Communication data that are not personal data are made openly accessible by default, as they are shared on the website and/or LinkedIn. They are discoverable through metadata, based on the medium they were published on.

4. Use case data containing personal data of citizens participating in INTERLINK and it is not planned to make them reusable. They were used to evaluate Interlinkers and the platform; they are closed by default. VARAM made some of its data available as open datasets on the Latvian Open Data Portal. Those datasets do not contain personal data.

5. Interlinkers: Interlinkers are available on the INTERLINK platform. They are searchable with the following meta-data : Name, Author, Last Update, Description, Nature, Problem Profiles, Rating and Keywords. Interlinkers will also be stored in Zenodo where they will be provided with a DOI and metadata.

2.2 Are the data produced and/or used in the project identifiable and locatable by means of a standard identification mechanism?

The data produced isbe identifiable and locatable by means of a standard identification mechanism.

The repository will provide a persistent identifier:

- every research object exported is assigned a persistent ID;
- DOIs are used to uniquely identify datasets and publications.

2.3 What naming conventions do you follow?

The names of folder and file are given in English. The following naming conventions will be used by INTERLINK members:

- each folder has a name that contains the identifier of the Work Package that supervises/uses this folder (e.g., WP1_name);
- each file contains at the beginning the identifier of the Work Package that supervise this file (e.g., WP1_name);
- when the file is a deliverable, the name contains the identifier of this deliverable (e.g., WP1_D1_name);
- when the file concerns a particular task, the name contains the identifier of the related task (e.g., WP1_T4_name);
- the folder/file name provides useful cues to the content (e.g., WP1_Guidance);
- the file name provides information about the status of the file (draft/final version) (e.g., WP1_T4_Assessment_draft);
- long file names are avoided.

2.4 Will search keywords be provided that optimize possibilities for reuse?

To optimize possibilities for reuse, INTERLINK provides search keywords such as:

- **fixed keywords**: "Collective awareness platforms", "Public sector innovation", "Technological innovation";
- **free keywords**: "New public governance", "Digital services", "Citizens participation", "co-production".

Interlinkers are attributed specific keywords, based on the purpose they serve (such as “survey”, “project management”, “analysis”, etc.).

2.5 What is your approach for clear versioning?

The versioning of folders and files is given in English. The following versioning conventions will be used by INTERLINK members:

- the name of the file contains the status of the file (draft/final version);
- the name of the file contains the last date of modification when the document needs to be updated by various partners (e.g., WP1_T6_guidance_draft_20.02.2020);
- the format date is: DD.MM.YYYY.

2.6 What metadata will be created?

The generated open data is discoverable with metadata and through a standard identification mechanism.

The repository (Zenodo, maintained by CERN) provides a persistent identifier, the Digital Object Identifier ("DOI") for the data. In addition, metadatas provide administrative information about the data (e.g., title, author, language, format, date, embargo period, publisher, license, access conditions, etc.).

Interlinkers on the INTERLINK platform are attributed the following metadata : **Name, Author, Last Update, Description, Nature, Problem Profiles, Rating and Keywords.**

3 FAIR data: Making data openly accessible

3.1 Which data produced and/or used in the project will be made openly available as the default? If some data is kept closed provide a rationale for doing so.

The consortium participates in the Horizon 2020 Pilot on Open Research Data, following the principle of "as open as possible, as closed as necessary". It adheres to a policy of open access to all project results, guidelines and reports.

In this DMP, the data collected and/or generated by INTERLINK are classified into four categories: internal management data (1), research data (2), communication data (3) use case data (4) and Interlinkers (5). Answers below are broken down among those categories.

1. Internal management data are not usable by third parties and were not made openly available by default.

2. Research data generated by the project have been made fully reusable.

3. Communication data that are not personal data have been made openly accessible by default.

4. Use case data containing personal data of citizens participating in INTERLINK and were not made reusable. They were primarily used to evaluate Interlinkers and the platform, and it has been decided to keep them closed by default. VARAM will make some of its data available as open datasets on the Latvian Open Data Portal. Those datasets will not contain personal data.

5. Interlinkers will be made available through the INTERLINK demo platform, accessible from the INTERLINK website.

3.2 How will the data be made accessible?

Data are available through different channels, depending on the data:

- concerning open access to peer-reviewed scientific publications and deliverables, "green" open access is the preferred option, with partners publishing in peer-reviewed scientific journals and then self-archiving a copy in the repository (Zenodo).
- Technical reports and other communicative documents have also archived in a free repository compatible with the requirements of "green" open access.
- all relevant information and textual material from the platform textual material (papers, deliverables, etc.) are also freely accessible on the project website.
- Interlinkers are available on the INTERLINK demo platform, accessible through the INTERLINK website.

3.3 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)?

The use of open-source software have been privileged when possible.

All artefacts published openly areaccessible via HTTP.

INTERLINK has used GitHub repository and published datasets in Zenodo.

Commonly used softwares in certain cases are needed to access the data (e.g., PDF, Excel, Word, PowerPoint).

3.4 Where will the data and associated metadata, documentation, and code be deposited? Have you explored appropriate arrangements with the identified repository?

The data, associated metadata, documentation and code have been deposited in Zenodo and/or on the INTERLINK demo platform.

3.5 If there are restrictions on use, how will access be provided?

Where there must be restrictions on use of certain data, access have been restricted/conditioned using a Data Sharing Agreement which specifies the conditions of access.

At the moment, no restrictions are in place.

4 FAIR data: Making data interoperable

4.1 Are the data produced in the project interoperable? What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?

The data produced are provided in non-proprietary or open standard, and lossless file formats.

The data produced arediscoverable through metadata by means of a standard identification mechanism.

The repository providesa persistent identifier, the Digital Object Identifier for the data.

In addition, metadata provides administrative information about the data (Title, author, language, format, date, embargo period, editor, license, access conditions, etc.).

The metadata have beengenerated by the repository or directly through the Internet platform.

4.2 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?

Standard vocabularies have been used for all data types present in INTERLINK dataset to enable interdisciplinary interoperability.

The data are well described to be reusable.

Among other things, the e-government core vocabularies handbook provided by the European Commission have been relied on:

https://ec.europa.eu/isa2/sites/isa/files/e-government_core_vocabularies_handbook.pdf

INTERLINK has generated project-specific vocabularies, in terms of creating "Interlinkers".

The specific vocabularies generated by INTERLINK are consistent with existing ontologies and will be reusable in the context of the co-creation and the co-delivery of services between public administrations and private stakeholders.

5 FAIR data: Increase data re-use (through clarifying licenses)

5.1 How will the data be licensed to permit the widest re-use possible?

Most of the INTERLINK deliverables have been made available for use and download on the INTERLINK website under a Creative Commons license.

Regarding to Interlinkers, and in order to disseminate the results in accordance with the Open Access rules and commitments, while respecting the intellectual property rights of the partners, the following strategy is applied :

By default, software Interlinkers are open-source under the Apache 2.0 license. Those components can be reused by respecting the requirements sent out by the Apache 2.0 license (https://www.apache.org/licenses/LICENSE-2.0)

By default, knowledge Interlinkers are open-source under Creative Commons CC BY-SA 4.0 (Attribution - Share Alike). Those Iinterlinkers can be reused by respecting the requirements sent out by the Creative Commons license. (https://creativecommons.org/licenses/by-sa/4.0/).

Specific software Interlinkers depend on the INTERLINK Co-Exploitation License and may require prior authorization before reuse. A complete list of internal Interlinkers can be found in Annex 6. More information on the INTERLINK Co-Exploitation License can be found in Deliverable 2.5.

5.2 When will the data be made available for re-use? If applicable, specify why and for what period a data embargo is needed.

No data embargo is envisaged. All the data that was planned to be shared is publicly available, either on the INTERLINK website (for deliverables and research data) or on the INTERLINK platforms (for Interlinkers).

5.3 Are the data produced and/or used in the project usable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why.

In this DMP, the data collected and/or generated by INTERLINK are classified into four categories: internal management data (1), research data (2), communication data (3), and use case data (4). Answers below are broken down among those categories.

1. Internal management data are not usable by third parties and were not made openly available by default.

2. Research data generated in the context of the project have been made fully reusable by third parties.

3. Communication data that are not personal data are reusable by third parties.

4. Use case data containing personal data of citizens participating in INTERLINK and were not made reusable. They were primarily used to evaluate Interlinkers and the platform, and it has been decided to keep them closed by default. VARAM will make some of its data available as open datasets on the Latvian Open Data Portal. Those datasets will not contain personal data.

5. **Interlinkers** are reusable by third parties, in respect of the specific licenses pertaining to each individual Interlinker.

5.4 How long is it intended that the data remains re-usable?

No deadline is fixed for the reusability of the data.

The INTERLINK website and INTERLINK demo platform will remain available for a year after the end of the project.

5.5 Are data quality assurance processes described?

Each INTERLINK partner is responsible for assuring the quality of the data it has produced and generated. The Consortium has relied on the following methods to ensure high quality of data :

- quality control measures during data collection : (1) review of collected data by appropriate INTERLINK members, (2) use of standardized data collection methods and protocols to ensure that collected data are not altered/changed, (3) use of standardized interview forms and checking consistency of responses.
- quality control measures during digitization, entry or coding of data : (1) the use of standard vocabularies, (2) the use of structured and/or purpose-built databases to organize data and data files (e.g., standardized Excel files, etc.).
- quality control measures for transcription of data : (1) the transcriptionist's commitment to full transcription of pertinent data when transcribing audio data into written data

6 Allocation of resources

6.1 What are the costs for making data FAIR in your project? How will these costs be covered?

The costs for making data FAIR in the project are covered by the funding allocated to INTERLINK. They are minimal.

Following the end of the project, FBK will bear the costs of maintening the INTERLINK website and demo platform online for one year. Deusto will continue the maintenance of the INTERLINK demo platform for one year.

6.2 Who will be responsible for data management in your project?

Each individual partner was responsible for its own data management.

Relying both on the Consortium Agreement signed early at the project's start by all beneficiaries, as well as on the close and long-lasting collaborations among some of the partners, all the partners proof they have adopted sufficient protection measures and policies providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject

Detailed information regarding the privacy related roles and responsibilities in INTERLINK can be found in Annex 3 "PRIVACY AND DATA PROTECTION – ROLES AND RESPONSABILITIES"

In the context of Use Cases, the Data Controllers respectively were ZGZ, MEF and Varam, while FBK and DEUSTO acted as Data Processors in their duty to processing the users' feedbacks in a pseudo-anonymized way on behalf of the three Data Controllers.

In the context of the website and newsletter development as well as communication manager, the Data Controller was DEDA, while FBK acted as Data Processor in its duties of hosting the website and providing technical maintenance of the newsletter.

In the context of platform development, the Data Controller was Tree Technology.

In the context of the explorative part of the use case analysis, the Data Controller was Radboud University.

In the context of Internal Data Management, the Data Controller was FBK in its capacity of Project Coordinator and in its duty to collecting and hosting the personal data of the other partners.For each data processing activity including more than one partner, all partners have reviewed and accepted Annex 4 "Data Processing Agreement" as a binding agreement between Data Controllers and Data Processors pursuant to art. 28 of the GDPR.

Following the end of the project, FBK will act as a data processor regarding the use of the INTERLINK platform. Each partner relying of the platform will act as a data controller for its own activities, as stated in the Post Project Agreement.

More information regarding the privacy related roles and responsibilities in the INTERLINK project can be found in Annex 3.

However, WP6 members played a central role in providing guidance on the applicable framework to the INTERLINK Project in that regard. Alain Strowel, the leading partner of WP6, is an academic and recognized expert in the field of data protection and oversees the data management aspects of INTERLINK. He can be contacted at alain.strowel@uclouvain.be. In addition, Jean De Meyere is WP6's main point of contact and can be contacted at jean.demeyere@uclouvain.be.

During the project, WP6 members provided input, shared amongst the partners. In relation to the processing of personal data, each partner relied on the assistance of their Data Protection Officers (DPO), as planned by their internal privacy policies. Anna Benedetti is the DPO of FBK, which manages the INTERLINK project. Anna Benedetti can be contacted at privacy@fbk.eu. The relevant privacy contacts for each partner can be found in Annex 1 of this document. The complete list of privacy policies can be found annexed to this document. A list of those policies can be found in Annex 2 of this document.

6.3 What are the costs and potential value of long-term preservation?

The costs of long-term preservation are minimal, as the data generated in the context of the project is in the order of several GB.

The potential value lies in the generated research data, defining a governance model based on co-production of public services.

Interlinkers are valuable for potential users of the INTERLINK demo platform during the year following the project.

7 Data security

7.1 What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?

The INTERLINK project partners do not conduct activities or produce outputs that raise any large-scale security issues. The project does not have the potential for military applications and does not involve the use of elements that may cause harm to humans, animals, plants or the environment. However, the process of collecting, processing and storing data could have some pitfalls. In order to reduce the risk of possible malicious, criminal and/or terrorist misuse, which could also be committed by malicious persons authorized to access the information, INTERLINK relied on a twofold security strategies :

- by ensuring that the security layers and privacy measures in place are functioning properly, by maintaining access logs, and by following best practices for system management;
- by using techniques to prevent information leakage "on-the-fly", i.e., by applying the aggregation and pseudonymization approach of personal and sensitive information at the time of collection, communication, and storage (e.g., via an encryption scheme, hash functions, and/or tokenization). In the unlikely event of a successful retrieval, such an approach,, neutralize eavesdropping and/or similarly dangerous hacking attempts by securing the data and rendering it completely meaningless to the potential attacker.

INTERLINK data are in the Zenodo repository or on the INTERLINK website or on the Google Drive and are protected through the adoption of appropriate technical and organizational security measures. Datasets containing personal data needs to be anonymized before being uploaded on Zenodo.

The project management data, the research data, and the communication data collected and/or generated by INTERLINK partners are processed in accordance with the standard best practices of each partner.

The use case data are securely stored at the premises and/or on the devices of the public institutions involved in their collection. Data security is be ensured by those public institutions, in compliance with their legal obligations. Use case partners have not transfer sensitive data to INTERLINK partners.

8 Ethical aspects

8.1 Are there any ethical or legal issues that can have an impact on data sharing?

Key ethical issues concerning research activities were examined from the INTERLINK point of view and included participant recruitment, participant information, informed consent, and data handling during planned research activities. The project activities were carried out taking into account ethical implications and respecting the rules expressed in international, European, and national texts and applicable codes of practices in force, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC ("General Data Protection Regulation").

Each INTERLINK partner ensured that personal data were processed in compliance with the General Data Protection Regulation, with the assistance of WP6 and FBK as project manager (WP1). In the context of use cases, INTERLINK established processes (e.g., obtaining consent, data retention policy, etc.) and documentation in compliance with the General Data Protection Regulation. Deliverable 6.5 Template Documentation for EU Privacy Compliance contained information regarding the information of data subjects regarding the processing of their personal data throughout the INTERLINK project. It was updated throughout the lifecycle of the project to ensure a safe and lawful processing of personal data throughout the project.

In this regard, use cases only involved voluntary participants, who were informed of the nature of their participation and the data collection and retention procedures through an informed consent form prior to commencing their participation. IInformed consent followed procedures and mechanisms consistent with European and national regulations in the field of ethics, data protection, and privacy. INTERLINK relied on its Privacy Policy and Consent Form (see Annex 5 of this document) to inform and collect consent from data subjects.

In addition, the following measures were foreseen:

- All possible data management precautions (such as encryption, authentication, and authorization) were taken to ensure data protection requirements (confidentiality, integrity, and availability).
- Appropriate administrative procedures were followed (including the involvement of the EAB and national Data Protection authorities, if necessary).
- Researchers were trained in the application of procedural safeguards.

Sensitive personal data were not processed in relation with the INTERLINk project. As such, this does not allow us to evaluate the inclusion of vulnerable groups throughout the INTERLINK project. However, such possibility was foreseen in the above-mentionned privacy documentation regarding health-data and migrant status, based on the request for explicit consent. A strategy was therefore in place to promote inclusion for participants, notably based on thefollowing Commission's guideline concerning the gender and migrant status of individuals : https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-refugees-migrants_en.pdf and en-guidelines-improving-collection-and-use-of-equality-data.pdf (europa.eu).

9 Other issues

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

None were reported by the MEF and VARAM use cases. The ZGZ use case will make use of the Spanish National Scheme of Data Security (ENS).

Annex 1 : Privacy Contacts

	Name	Email address	Phone contact
CNS	Olli Pelkonen	privacy@cloudnsci.com	N/A
DEDA	Andrea Reghelin	dpo@dedagroup.it	N/A
DEUSTO	Mikel García Llorente	dpo@deusto.es	+34 944139430
FBK	Anna Benedetti	privacy@fbk.eu	+39 0461314370
MEF	Maria Laura Ferrigno	marialaura.ferrigno@mef.gov.it	N/A
RU	Francie Manhardt Ellen K. Nieboer	francie.manhardt@ru.nl ellen.nieboard@ru.nl	+31 6 272 85 063 +31 6 31 1132 785
TREE	Écija	dpo@treetk.com	N/A
UCL	Michèle Rémy	privacy@uclouvain.be	N/A
VARAM	Martins Verdins	das@varam.gov.lv	+ 371 67026502
ZGZ	Fernando Tirado Aznar	dpd@zaragoza.es.	+34976721801

Annex 2 – List of the privacy policies

	Document Number	Link (if available online)
DEDA	Annex 2.1	Link
DEUSTO	Annex 2.2	Link
FBK	Annex 2.3	Link
MEF	Annex 2.4	Link [ITA]
RU	Annex 2.5	Link
TREE	Annex 2.6	N/A
UCL	Annex 2.7	Link
VARAM	Annex 2.8	Link [LAV]
ZGZ	Annex 2.9	N/A

Annex 3 – PRIVACY AND DATA PROTECTION - ROLES

What kind of handling of personal data were realized during the project?

1. WEBSITE AND NEWSLETTER (hosting, content development, management of mailing lists, dissemination activities, contacts)
2. USE CASES (recruitment of volunteers, interviews, questionnaires, focus groups
3. Co-creation platform (requirement collection; backend; maintenance; personal account creation; evaluation)
4. Internal management data [Data of the partners (database)]

PRIVACY ROLES OF PARTNERS:

ROLE	PURPOSE OF DATA PROCESSING	PARTNER/S
DATA CONTROLLERS	1)	DEDA
	2)	ZGZ
	2)	MEF
	2)	RU
	2)	VARAM
	3)	TREE
	4)	All partners
DATA PROCESSORS	12) + 4)	FBK
	2)	DEUSTO

As regards purposes 2 and 4, all partners agreed to consider Annex 4 as the Data Processing Agreement between Data Controllers and Data Processors.

ROLES OF PARTNERS

Partner	**Purpose of Data processing**	**Type of data processed**	**People involved**	**Processing mode**	**Data sharing** (to whom and how)
FBK	1. website hosting	No tracking of personal data. Only technical cookies.	Website users	Microsoft Azure to host the site (sub-responsible already appointed by FBK)	Dedagroup
	2. Processing of users'	Socio-demographic information (age, gender, job,	Volunteers participating in the UCs	Pseudo-anonymized data	MEF, ZGZ e VARAM

	feedback from use cases	nationality) and results of questionnaires, interviews, focus groups		received from MEF, ZGZ, VARAM	
	4. Internal data Management	Name, contact details, cost of personnel	Project partners	Google Share Drive to host the data received from all partners	European Commission
Dedagroup	1. Website: Development, content management	Only technical cookies	Website use	Through FBK	None
	2. Newsletter setup	Name, email	Newsletter subscribers	Sendingblue	None
	1. LinkedIn website	Pictures	INTERLINK project members and use case participants	Informed consent form	None
MEF	2. Recruitment of volunteers to use the platform	Socio-demographic information (age, gender, job, nationality)	Volunteers participating in the UC	Informed consent Google Form	None
	2. Questionnaires	Socio-demographic information (age, gender, job, nationality) and email	Volunteers participating in the UC	Informed consent Google Form	FBK, Deusto (?), Tree Technology (?) (pseudo-anonymized)
	2. Interviews, focus goups	- Socio-demographic information (age, gender, job, nationality) - Audio/videos of interviews/focus groups	Volunteers participating in the UC	(Video) Recording of (virtual) session (videoconference systems; recording systems	FBK, Deusto (?), Tree Techonology (?) (pseudo-anonymized)
ZGZ	2. Recruitment of volunteers to use the platform	Socio-demographic information (age, gender, job, nationality)	Volunteers participating in the UC	Informed consent Google Form	None

	2. Questionnaires	Socio-demographic information (age, gender, job, nationality) and email	Volunteers participating in the UC	Informed consent Google Form	FBK, Deusto (?), Tree Technology (?) (pseudo-anonymized)
	2. Interviews, focus goups	- Socio-demographic information (age, gender, job, nationality) - Audio/videos of interviews/focus groups- Personal data (name, sex, age - Audio/videos of interviews/focus groups	Volunteers participating in the UC	(Video) Recording of (virtual) session (videoconference systems; recording systems	FBK, Deusto (?), Tree Techonology (?) (pseudo-anonymized)
VARAM	2. Recruitment of volunteers to use the platform	Socio-demographic information (age, gender, job, nationality)	Volunteers participating in the UC	Informed consent Google Form	None
	2. Questionnaires	Socio-demographic information (age, gender, job, nationality) and email	Volunteers participating in the UC	Informed consent Google Form	FBK, Deusto (?), Tree Technology (?) (pseudo-anonymized)
	2. Interviews, focus goups	Socio-demographic information (age, gender, job, nationality) - Audio/videos of interviews/focus groups	Volunteers participating in the UC	(Video) Recording of (virtual) session (videoconference systems; recording systems	**FBK, Deusto, Tree Techonology** (pseudo-anonymized)
Tree Technology	3. Personal account creation to access the cocreation platform	Socio-demographic information (age, gender, job, nationality) Username and password	Platform users	N/A	N/A

	3. Assessment of the platform	Results of questionnaires	Platform users	Pseudo-anonymized (answers associated to a code)	N/A
Radboud University	2.Explorative part of the use case analysis	Resulsts of questionnaire	INTERLINK project members	Audio recordings and transcripts shared au Surfdrive	N/A
DEUSTO	2/ Processing of users' feedback from use cases	-Socio-demographic information (age, gender, job, nationality) - Audio/videos of interviews/focus groups	Volunteers participating in the UCs	Pseudo-anonymized data	MEF, ZGZ, VARAM

Annex 4 – DATA PROCESSING AGREEMENT PURSUANT TO ART. 28 OF THE GDPR AND PROVISION OF INSTRUCTIONS

Art. 1 - Object

In accordance with and pursuant the effects of article 28 of the GDPR, the Partners indicated as Data Controllers in Annex 3, as "*Data Controllers*", hereby appoint the Partners indicated as Data Processors in Annex 3 as "*Data Processors*" after having them found suitable for the role, and give hereafter the obligations that the latter are required to comply with in reference to the processing made on behalf of the Data Controllers. The Processors will carry out all the processing operations necessary for the execution of the assignment pursuant to the Interlink Project as detailed in Annex 3.

Therefore, the Processors commit to the rigorous respect – with due diligence appropriate to the matter – of the aforementioned EU legislation, of its corresponding national legislation, as well as the provisions of the National Data Protection Authorities (hereinafter "Authority"), the Article 29 Working Party and the European Data Protection Board.

Without precluding any additional liability towards the Data Controllers, it is hereby understood that any type of determination of the purposes and/or of the means of the processing made from the Processors implies the assumption of the title of Data Controllers of the processing, with all its additional consequences.

Art. 2 - Description of the Processing

The Processor is authorised to process on behalf of the Data Controller only the personal data necessary for the execution of the processing as described in D.6.2 - Data Management Plan (point 6.2 and Annex 3).

Art. 3 - Data Controller's obligations

The Data Controller finds that the personal data that has transferred and will transfer to the Processor are relevant and not exceeding the purpose for which they have been collected and then processed, and that they are gathered and transferred in accordance with all requirements of the applicable law.

It is the Data Controller's responsibility to find the legal basis for the personal data processing.

Art. 4 - Data Processor's obligations

At every stage and for every operation of the processing, the Processor must guarantee the respect of the EU principles (such as *privacy by design* and *by default*) and the national ones in the field of personal data protection. Specifically, the Processor must:

a) Assist the Data Controller with adequate technical and organisational measures, in order to comply with the Data Controller's duty to follow-up on any information requests made by data subjects, by informing the Data Controller as soon as possible about the received complaints from the data subjects;

b) Provide the Data Controller with all the necessary information in order to demonstrate compliance with the current appointment, allowing and contributing for the revision activities, including inspections, undertaken by the Data Controller or by its Data Protection Officer, or by another subject so commissioned;

c) Assist the Data Controller in ensuring the compliance with obligations provided for by the articles 35-36 of the GDPR. Specifically, with regards to the establishment of a *Data Protection Impact Assessment*, if the Data Processor supplies the Data Controller with means/software and/or manages them whilst they belong to the Data Controller, the Data Processor will be obliged to provide and update the risk analysis (probability of a security violation) of the means/software, and notify the Data Controller in compliance with the criteria given by the latter;

d) Inform the Data Controller whenever, in its opinion, an instruction violated the Regulation or other provisions, nationals or EU, relating to the protection of personal data;

e) Comply with the provisions coming from the Authority and collaborates with the Data Controller in order to implement the provisions it has been given;

f) Assist the Controller in its defence during litigation before the Authority, on the Data Controller's request and expenses;

g) Proceed to appoint a Data Protection Officer (hereinafter, "DPO"), in the cases provided for by the article 37 of the GDPR, and in accordance with the criteria for selection set out by the GDPR, of its related guidelines of Article 29 Working Party, as well as the instructions provided for by the Authority, warranting for the compliance with the provisions referred to in article 39 of the GDPR;

h) Provide for the arrangement of the Record of Processing Activities as provided for by article 30 of the GDPR, keeping it at the disposal of the Data Controller, or the Authority, if requested to do so.

Art. 5 - Safety Measures

The Data Processor must take safety measures and guarantee the confidentiality of personal data in order to minimize the risks of destruction, of intentional or accidental loss of data and unauthorized access, in compliance with the EU and national law principles in the field of personal data protection and, specifically, those provided for in the Articles 5 and 25 of the GDPR. Notably the Processor guarantees a level of protection appropriate for the risk exposure, as provided for in article 32 of the GDPR.

Art. 6 - People authorized to process personal data

The Data Processor must comply with the instructions given by the Data Controller.

The Processor guarantees that people processing personal data have been specifically authorized, properly trained and are committed to confidentiality, or that they have a proper legal duty of confidentiality. Following below is a list of instructions that the Processor must give to those authorized to process personal data together with the aforementioned Regulation (hereinafter "Authorized Processor"):

a) Do not take any action on personal data if not authorized by specific legislative provisions or by other legal grounds applicable pursuant to the legislation, such as the data subject's consent. Whenever this circumstance is uncertain, the Authorized Processor must contact the Processor to obtain the necessary confirmation; the processing operations carried out must be relevant and not exceeding the purposes for which the data has been collected;

b) The processing of information and personal data with which the Authorized Processor comes into contact for work reasons is made strictly to carry out the institutional activities with the utmost confidentiality towards the outside and the internal world. In no way should personal data be disclosed or communicated to third parties without the prior authorisation of the Data Controller;

c) Take security measures in accordance with article 32 GDPR, in reference to data processing carried out both through electronic devices and without them, and specified by the Data Controller on a case-by-case basis, while reporting to the latter the potential risks of destruction or loss (even accidental) of personal data, as well as unauthorized access, non-consensual processing and processing that doesn't comply with the purposes of the collection;

d) Take the necessary precautions to ensure the confidentiality of the given credentials, and the diligent preservation of devices at their own use and possession;

e) Verify the accuracy and integrity of the collected and processed data and, where necessary, provide for their relative rectification and update;

f) Participate to the training courses organised by the Data Processor or the Data Controller with regards to data protection;

g) Notify the Processor about any information that is considered relevant with reference to personal data processing.

Further and more specific instructions, on account of the type of processing, will be given time and again to the Authorized Processor by the Data Processor. The Processor will inform the Authorized Processor that for any uncertainty concerning the accuracy of a processing operation, they must address their direct Supervisor who, if necessary, will proceed to engage with the Controller.

Finally, the Authorized Processor must be informed that complying with the duty of diligent and proper execution of the received information could provide for an element of evaluation of the work carried out as part of their contractual agreement with the Processor.

Art. 7– Resorting to other Processors

The Data Controller, with this Act of Appointment, confers the general written authorisation to the Processor to resort to any additional Data Processors (hereinafter "sub-Processors") if necessary for the execution of specific processing activities on behalf of the Data Controller, without any further specific authorisation having to be issued by the Controller.

The Controller commits to making the sub-Processors sign a contract or another legal document, as provided for in article 28, par. 4 of GDPR, which imposes on the latter the same obligations in the field of personal data protection as laid down in this document, and providing for sufficient guarantees for implementing technical and organisational safety measures appropriate for pursuing the requirements provided for in the GDPR.

It is agreed that, where the sub-Processor omits to comply with their obligations in the fields of personal data protection, the Processor will be held responsible towards the Controller for the compliance with the obligations of the sub-Processor.

Art. 8 - Place of processing and data transfer towards third countries

Personal data will be processed within the European Economic Area (EEA). Should they be transferred to Third Countries, in the absence of an adequacy decision from the European Commission, the Processor will undertake additional measures in order to guarantee a level of protection equivalent to the one offered in the EEA, and will respect the provisions set out by the applicable legislation on personal data transfer towards Third Countries, such as Standard Contractual Clauses provided by the European Commission.

Should the legislation, EU or national, require the Processor to transfer personal data towards a Third Country or an international organisation, the Processor must inform the Controller of such requirement, unless said legislation forbids such information on grounds of public interest.

Art. 9 - Data Breach and Reporting Procedure

The Processor commits to assisting and supporting the Controller in the compliance with the obligations concerning personal data breach. Notably, the Data Processor commits to promptly reporting any violation (real or potential) that could reasonably involve personal data processed on behalf of the Data Controller.

The notification must be made in written form, and must have the elements referred to in Article 33, par. 3 GDPR and it must be submitted without undue delay together with any useful documentation, to the Data Controller in order to allow for a notification to the Authority, if necessary, and for a potential communication to the data subjects.

Art. 10 - Erasure of personal data

Upon request from the data Controller, on the expiration date of the contractual relationship above or at the end of the execution of the related activities/performances, the Processor will delete the personal data that was processed and every existing copy, unless they are to be further preserved in accordance with existing law or additional compatible purposes.

In the case of automated processing, the Processor guarantees that, upon a request from the Controller and without additional costs, before deleting the data, will be able to carry out a safe transfer of data to another subject, in a structured format, of common use and in a machine-readable form, if the receiver is authorized to receive them.

Art. 11 - Indemnity

In case of a civil legal action, or of administrative liability, brought against the Controller for damages caused or for violations committed by the Processor following a failure to comply with legislation or with contracts, the Processor completely indemnifies the Controller, without exception.

Similarly, the Processor completely indemnifies the Controller, without exception, in case of application of penalties by the Supervisory Authority concerning the Processor and/or the sub-Processor's failure to comply with legislation or with contracts.

Art. 12 - Duration

This act of appointment is valid since the start date of the Interlink Project until its every effect has ceased - including possible renewal, deferral, additions or extension of the same - related to the services provided by the Processor on behalf of the Controller.

Art. 13 - Final provisions

Should any dispute or claim arise in connection with this act of appointment, the Parties agree on the jurisdiction of the courts of Luxembourg settle them.

Additional changes to the present act of appointment must be approved through a written agreement between the Parties.

Annex 5 – PRIVACY NOTICE AND CONSENT FORM

A. Interlink Privacy Policy

Privacy Notice of the **Interlink Project**

Type of personal data

General Data
We process general personal data about you.

More info can be found in section 6 of this Privacy Notice.

Health Data
We process your health data.

More info can be found in section 6 of this Privacy Notice.

Migrant Status
We process data related to your status as a migrant.

More info can be found in section 6 of this Privacy Notice.

Source of personal data

Provided Data
We process personal data that you provide to us.

More info can be found in section 7.1 of this Privacy Notice.

Collected Data
We process personal data that we collect about you.

More info can be found in section 7.1 of this Privacy Notice.

Purpose of processing

To evaluate and assess the impact of the INTERLINK solution.

We process your personal data to assess participation and understand the social impact of the project.

More info can be found in section 9 of this Privacy Notice.

Passing on to third parties

Data Transfers
We transfer your personal data to other members of the INTERLINK consortium.

More info can be found in section 7.5 of this Privacy Notice.

Place of processing

European Union
We **do not** process your personal data outside of the EU.

More info can be found in section 7.4 of this Privacy Notice.

1. Data controller

[To be completed for each use case: Zaragoza/MEF/VARAM]

2. The Interlink Project

INTERLINK is a European project whose goal is already apparent from its name: "Innovating goverNment and ciTizen co-dEliveRy for the digitaL sINgle market". More precisely the goal is to develop a new collaborative governance model that promotes the reuse and sharing of existing public services by leveraging on the partnership between citizens, private actors, and public administrations. The piloting of the INTERLINK solution in three European public administrations in Italy (MEF), Latvia (VARAM) and Spain (Ayuntamiento de Zaragoza) will enable the project to validate the effectiveness of the project results. Stakeholders involved in the three pilots were selected to assess their experience and interest in the co-production of public services, in particular in the INTERLINK co-production model and associated supporting tools.

The project activities will last 3 years, from 1 January 2021 to 31 December 2023. INTERLINK is coordinated by the Fondazione Bruno Kessler - FBK (Italy). Its consortium counts on a highly competent international team from 6 European countries (Belgium, Netherlands, Finland, Italy, Latvia and Spain). INTERLINK is a Horizon2020 research and innovation action (RIA) funded under the topic "DT-GOVERNANCE-05-2018-2019-2020 - New forms of delivering public goods and inclusive public services" programme.

3. Voluntary Participation

Participation is not compulsory. You can decide for yourself whether you want to participate in the project INTERLINK or not. If you decide to participate, you will receive this privacy policy to keep and will be asked to sign a consent form and/or tick a box to indicate your agreement. You can withdraw your participation at any time and without giving any reason, without this affecting the benefits to which you are entitled or having any negative consequences.

4. What are the possible disadvantages or risks of taking part?

No risks are foreseen. You are only requested to be available to participate. All information provided will be treated with the highest confidence.

5. The MEF/VARAM/Zaragoza Use Case

The Ministry of Economy and Finance - Italy (acronym: MEF) has extensive experience in bottom-up collaboration approaches and is always looking for ways to further develop its expertise and stay at the forefront of innovation.

To this end, MEF has decided to participate in INTERLINK and develop a model of a Participatory Strategic Planning Module (PSPM) that will allow public institutions and their staff to actively participate in the definition of MEF's strategic plan and access a collection of best practices on strategic planning approaches and methodologies.

VARAM, the Ministry of Environmental Protection and Regional Development of the Republic of Latvia (https://latvija.lv/ EN), is a portal that provides easy access to the services of state and local government institutions. Its aim is to constantly update and improve this portal so that the published public services are more and more accepted.

The City of Zaragoza (ZGZ) and its Centre for Arts and Technology (eTOPIA_) aim to promote collaborative urban design facilities and programs and improve the process of open innovation in the city.

6. Types of data collected

The following personal data will be collected during the course of the INTERLINKproject:

- Name
- Address
- Email
- Phone number
- Age
- Gender
- Picture
- Education level
- Professional field and status
- Migrant status
- Activity while using the Interlinkers (e.g. logs)
- Other (please specify)

Personal data regarding any disability you may have will be collected as part of the INTERLINK project.

No personal data of data subjects under 13 years old will be collected as part of the INTERLINK project.

7. Methods and place of processing of personal data

7.1 Methods of processing

The data controller shall take appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the data. The data processing is carried out using computers and/or IT enabled tools, following organizational procedures and modes strictly related to the purposes indicated.

7.2 Collection of data

We collect your personal data directly from you when you are participating in the INTERLINK project.

Some data (logs) will be collected directly when you use our Interlinkers.

7.3 Legal basis of processing

The data controller may process your personal data if one of the following applies:

- You have given your consent for one or more specific purposes.

- processing is necessary for the performance of an agreement with the participant and/or for any pre-contractual obligations thereof;
- processing is necessary for compliance with a legal obligation to which the data controller is subject;
- processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the data controller;
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party.

All of the personal data processed throughout the INTERLINK project will rely on your consent. Your consent will be recorded through the signing of a consent form. You have the right to withdraw his consent to any further processing at any time.

7.4 Place of the processing

Your personal data is processed at the data controller's operating offices and in any other places where the parties involved in the processing are located.

Depending on your location, data transfers may involve transferring your personal data to a country other than their own. personal data may be processed in Italy, Spain, the Netherlands, Finland, Belgium, Latvia and any other country of the European Union. No personal data will be transferred outside of the European Union.

7.5 Transfer of personal data

Your personal data may be transferred to and processed by other members of the INTERLINK consortium. Those are:

- The Fondazione Bruno Kessler (BK), a research center in Italy;
- The University of Deusto, in Spain;
- Tree Tech SA, an R&D SME in Spain;
- Rabout University, in the Netherlands;
- Cloud'N'Sci Ltd, a tech start-up in Finland;
- The Université Catholique de Louvain, in Belgium ;
- Dedagroup Public Services in Italy,
- The Italian Ministry of Economy and Finance;
- The Ministry of Environmental Protection and Regional Development of the Republic of Latvia; and
- The city department of Zaragoza in Spain.

More information regarding other members of the INTERLINK consortium can be found at the following address: https://interlink-project.eu/partners/.

8. Retention time

Personal data shall be processed and stored for as long as required by the purpose they have been collected for.

The data controller may be allowed to retain personal data for a longer period whenever you have given consent to such processing, as long as such consent is not withdrawn. Furthermore, the data controller may be obliged to retain personal data for a longer period whenever required to do so for the performance of a legal obligation or upon order of an authority.

Once the retention period expires, personal data shall be anonymized and deleted. Therefore, the right of access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after expiration of the retention period.

The retention period will run until the end of the INTERLINK project in January 2024.

9. Purposes of processing

Your personal data is collected to allow the data controller to provide its service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests (or those of its participants or third parties) and detect any malicious or fraudulent activity.

Personal data will be processed for the following purpose:

- **to evaluate and assess the impact of the INTERLINK solution**: to achieve this objective, the project will process personal data from citizens to assess participation and understand the social impact of the project.
- **to verify user's participation in the INTERLINK project:** pictures will be taken in order to verify that you participated in INTERLINK meetings.
- **For marketing and communications purposes.**

10. Your rights

You may exercise certain rights regarding your personal data processed by the data controller.

In particular, you have the right to do the following:

- Withdraw your consent at any time. You have the right to withdraw consent where you have previously given their consent to the processing of your personal data.
- Object to processing of your data. You have the right to object to the processing of their data if the processing is carried out on a legal basis other than consent. During the course of the INTERLINK data, all data is processed based on your consent.
- Access their data. You have the right to learn if data is being processed by the data controller, obtain information regarding certain aspects of the processing and obtain a copy of the data undergoing processing.
- Verify and seek rectification. You have the right to verify the accuracy of their data and ask for it to be updated or corrected.
- Restrict the processing of your data. You have the right, under certain circumstances, to restrict the processing of your data. In this case, the data controller will not process your data for any purpose other than storing it.
- Have your personal data deleted or otherwise removed. You have the right, under certain circumstances, to obtain the erasure of their data from the data controller.
- Receive your data and have it transferred to another controller. You have the right to receive their data in a structured, commonly used and machine-readable

format and, if technically feasible, to have it transmitted to another controller without any hindrance. This provision is applicable provided that the data is processed by automated means and that the processing is based on your consent, on a contract which you are part of or on pre-contractual obligations thereof.

- Lodge a complaint. You have the right to bring a claim before their competent data protection authority.

10.1 Details about the right to object to processing

Where personal data is processed for a public interest, in the exercise of an official authority vested in the data controller or for the purposes of the legitimate interests pursued by the data controller, you may object to such processing by providing a ground related to their particular situation to justify the objection.

10.2 How to exercise these rights

Your request to exercise your rights can be directed to privacy@INTERLINK-project.eu. These requests can be exercised free of charge and will be addressed by the data controller as early as possible and within one month (with extensions for some cases).

11. Benefits of the project

You will make a significant contribution to the achievement of the main objectives of the INTERLINK project. The INTERLINK project can help simplify the e-services offered by public administrations and improve the way citizens and businesses interact with their local or national authorities.

12. Confidentiality

All the personal data collected during the course of the research will be kept strictly confidential. You will not will be able to be identified in any publications**.** The results of this investigation may be published in reports, scientific journals or conferences and used in further studies, but it will not be possible to identify the source of the information. None of the provided data will be handled by third parties. The authorization for the use and access to personal data is valid until the end of the project, unless you decide to withdraw for the project. Your decision whether or not to give your authorization for the use and diffusion of your personal data is completely voluntary.

13. Consent

Participation in this project is accepted on the basis that you freely and independently sign a consent form and/or tick a check box to indicate your consent, in order to authorize us to process your personal data.

14. Future change in privacy policy

We may modify this Privacy Policy from time to time to reflect changes to our processes. Any changes to this Privacy Policy will be communicated to you by email. You retain the right to withdraw your consent to the processing of your personal data at all times.

15. Dispute Resolution

Questions or complaints regarding the data collected, this privacy policy or other privacy matters can be addressed at INTERLINK consortium at the following address: privacy@INTERLINK-project.eu.

You can also contact the Data Protection Officer of Zaragoza/VARAM/MEF at the following address : dpd@zaragoza.es / das@varam.gov.lv / marialaura.ferrigno@mef.gov.it

You have the right to lodge a complaint to their national data protection authority :

Garante per la protezione dei dati personali
Piazza Venezia, 11
00187 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 785
Email: segreteria.stanzione@gpdp.it
Website: http://www.garanteprivacy.it/

data State Inspectorate
Elijas Street 17
LV-1050 Riga
Tel. +371 6722 3131
Fax +371 6722 3556
Email: pasts@dvi.gov.lv
Website: https://www.dvi.gov.lv/

Agencia Española de Protección de Datos (AEPD)
C/Jorge Juan, 6
28001 Madrid
Tel. +34 91 266 3517
Fax +34 91 455 5699
Email: internacional@aepd.es
Website: https://www.aepd.es/

II. INTERLINK Consent Form

Project: “INTERLINK: Innovating goverNment and ciTizen co-dEliveRy for the digitaL sINgle marKet”

1	I am 18 years or older and I am competent to provide consent.
2	I confirm that I have read and understand the INTERLINK privacy policy explaining the above-mentioned research project and its implication regarding the processing of my personal data. I have been fully informed about the aims and purposes of the Project INTERLINK. I have had the opportunity to ask questions and/or read FAQs about the project. I have been informed about my rights as a data subject and on the way I can enforce those rights.
3	I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason and without there being any negative consequences.
4	I understand that my data will be kept strictly confidential. I give permission for members of the research team to process the following personal data **to evaluate and assess the impact of the INTERLINK solution** (please tick the appropriate checkboxes): Name, Address, Email, Phone number, Age, Picture, Gender, Education level, Professional field, Professional status, Logs data [ ] Migrant status [ ] Health data (e.g. disability) [ ]
5	I understand that my data will be kept strictly confidential. I give permission for members of the research team to process **my picture in order to to verify user’s participation in the INTERLINK project.** **Yes [ ]** **No [ ]**

6	I understand that my data will be kept strictly confidential. I give permission for members of the research team to process **my picture for communication and marketing purposes** **Yes [ ]** **No [ ]**
7	Information may be shared between any of the other researcher(s) and partners participating in this project. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the publications that result from the research. I have no objection that my data is published in a way that does not reveal my identity, without my explicit consent. The researcher(s) will ensure to preserve my anonymity as much as technically possible.
8	I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the INTERLINK research team.
9	I agree to take part in the above research project.
10	I have received a copy of this agreement.

I do hereby agree and give my consent for the treatment of my personal data within the INTERLINK project.

□

____________________________	___________________	________________________
Name of participant	Date	Signature
--------------------------------------	-----------------------	------------------------------
Lead Researcher	Date	Signature