INTERLINK

WP6 Legal and Ethical Requirements

D6.6 – Report on legal requirements

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)	Jean De Meyere (UCL), Alain Strowel (UCL)
Editor(s)	N/A
Reviewers	Anna Benedetti (FBK, Ethics Advisory Board), Laura Somaini (Covington & Burling LLP, Ethics Advisory Board), Quentin Fontaine (Altius), Danilo Giampiccolo (FBK),
Leading Partner	UCL
Version	V1.0
Deliverable Type	R
Dissemination Level	PU
Date of Delivery	30.04.2023
Submission Date	31.05.2023

VERSION HISTORY

Version	Issue Date	Status	Changes	Contributor
0.1	19.04.23	Draft (v2)	Update to national legislation, introduction of Chapter 4 (DSA) and Chapter 5 (IP)	UCL
0.9	05.05.23	Prefinal	Internally revised version sent to the EAB	FBK, UCL
1.0	29.05.23	Final	EAB revised versions integrated, document finalized for submission	UCL, FBK

Table of contents

1. Introduction 6

1.1. Structure of the deliverable 6
1.2 Summary of INTERLINK objectives and activities 6

2. EU legislation applicable to INTERLINK activities 8

2.1 General Data Protection Regulation 8
2.1.1 Summary 8
2.1.2 Requirements for INTERLINK 10
2.1.3 Implementation of the requirements 11
2.2 Public Sector Information Directive ('Open Data Directive') 12
2.2.1 Summary 12
2.2.2 Requirements for INTERLINK 12
2.2.3 Implementation of the requirements 13
2.3 Rules applicable in the EU research and innovation framework programme (Horizon 2020) 13
2.3.1 Summary 13
2.3.2 Requirements for INTERLINK 14
2.3.3 Implementation of the recommandation 14
2.4 The Digital Services Act 14
2.4.1 Definitions 14
2.4.2 Obligations concerning INTERLINK as on online platform 16
2.4.3 Requirements for INTERLINK 18

3. National legislation applicable to INTERLINK activities 20

3.1 Italian legislation 20
3.1.1 Digital Administration Code 20
3.1.2 Three-Year Plan for IT in the Public Administration (2020-2022) 20
3.1.3 AgID Guidelines 21
3.1.4 Guidelines on the enhancement of public IT assets 22
3.1.5 Guidelines on the technical interoperability of Public Administrations and Guidelines on Technologies and standards for the security of interoperability through API of computer systems 22
3.1.6 Implications for INTERLINK 22
3.2 Latvian legislation 23
3.2.1 Digital Transformation Guidelines 2021-2027 23
3.2.2 Service Environment Development Plan 2020-2023 23
3.2.3 State E-services Regulation 23
3.2.4 Monitoring Framework for State Information Systems Development Projects 24
3.2.5 Municipalities Law 24
3.2.6 Implications for INTERLINK 24
3.3. Spanish legislation 25
3.3.1. Law on Citizen's Electronic Access to Public Services 25
3.3.2. Electronic Administration Ordinance 25
3.3.3. Zaragoza's open government platform 26
3.3.4 Implications for INTERLINK 26

4. Intellectual Property Considerations regarding co-delivery 27

5. Conclusion 28

Executive summary

This report aims to provide a structured and systematic overview of the legal framework applicable to the INTERLINK project. It covers the applicable EU law and the national laws of the Member States where the use cases will be implemented. This version of the report is final and is due at Month 28. However, subsequent changes in legislation might entail revision or addition to this report.

1. Introduction

1.1. Structure of the deliverable

This report will be divided into two main parts. The first part of the deliverable will describe the EU law relevant to the activities of INTERLINK. The GDPR and Open Data Directive will be covered, then the Framework Programme for Research and Innovation. The Digital Services Act is also considered as a source of regulation related to INTERLINK. The second part of the deliverable reports on the national laws of Italy, Latvia and Spain, as these are the Member States where the use cases are implemented. Finally, we offer first considerations on intellectual property on the INTERLINK platform.

For each of the legal acts covered, the report begins with a section summarising the main objectives and the principles enshrined therein. A second section then sets out the specific requirements for the INTERLINK project and its partners.

1.2 Summary of INTERLINK objectives and activities

Defining the objective and activities of the consortium is a mandatory first step in determining the applicable law. In the case of INTERLINK, the applicable law is defined by the data processing activities of the project. Therefore, the project's Data Management Plan (Deliverable 6.2) is worth reading in conjunction with this report.

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 citizens' initiatives with the legitimacy and accountability granted by top-down e-government frameworks. INTERLINK assumes that by implementing a public-private partnership that combines the bottom-up approach of citizens' initiatives with the top-down approach of traditional e-government frameworks, we can overcome the barriers that prevent public administrations from efficiently reusing, sharing and delivering services together.

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

- **Developing a new collaborative governance model** based on partnerships between public administrations, citizens and businesses. To achieve this goal, INTERLINK will collect data from public administrations, citizens and NGOs to assess their needs in terms of governance models and analyse current and/or planned partnerships.

- **Providing a set of Interlinkers** (i.e., digital building blocks that standardise the basic functions needed by private actors to co-produce a service) to remove technological barriers and promote the delivery of interoperable, inclusive, sustainable and ethical public services. To achieve this goal, INTERLINK will collect data from private actors related to public services.

- **Providing the INTERLINK framework and operational platform** based on an open software system accessible through web and mobile connectivity to facilitate the co-production of services between public administrations and private actors. To achieve this goal, the project

will collect data from public administrations and private actors to identify their needs in terms of co-production of services. The data collection will allow us to understand what is already in place and what could be created. The data obtained will relate to service providers and services.

- **Identifying the legal framework for co-production and co-provision of services** to ensure that INTERLINK frameworks and governance models are in line with EU law and can be used for cross-border services. To achieve this objective, the project will collect data on the regulation of activities carried out by INTERLINK and its stakeholders (including use case members).

- **Evaluating and assessing 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 goal, the project will collect data from citizens, businesses, public administrations and other stakeholders for each use case. This data will be analysed to assess citizen participation and understand the social impact of the project.

To make the project objectives measurable and validate the project approach, INTERLINK foresees the development and implementation of three use cases within the three public administrations of the consortium: the Italian Ministry of Economy and Finance (MEF), the Latvian Ministry of Regional Development (VARAM) and the City of Zaragoza (ZGZ).

INTERLINK will collect/produce data divided into four categories:

- **Internal administrative data**: Data shared between individual consortium members or representatives of partner institutions to manage and coordinate the project.

- **Research data**: Data collected as part of academic research at Radboud University (WP2) on governance models and UCL (WP6) on legal requirements.

- **Communication data**: Data processed to update the website and communicate about project activities.

- **Use case data**: Data collected within the three use cases in the city of Zaragoza (Spain), the municipality of Reggio Emilia (Italy) and Latvia. The Interlinkers developed within WP3 led by FBK will contribute to the data collection. It will contain personal data of the participants and will be used to monitor the performance of the project.

In view of the above, the legal framework applicable to the INTERLINK project consists mainly of the legislation on the processing of personal data. As public administrations are involved in the project as stakeholders, the laws relating to data held by public sector bodies are also part of the legal framework applicable to the project. Finally, the rules applicable to the EU research and innovation framework programme apply.

2. EU legislation applicable to INTERLINK activities

2.1 General Data Protection Regulation

2.1.1 Summary

The General Data Protection Regulation (GDPR), which came into force on 25 May 2018 and replaced all previous European personal data protection laws, regulates how organisations handle personal data. It was created to keep up with the new digital world, protect EU citizens' rights to privacy and security, and ensure a common approach to data protection across Europe.

The GDPR gives data subjects more control over how their personal data is handled than previous data protection regulations and sets higher standards for organisations that process and manage personal data. It also empowers supervisory authorities - the regulators responsible for each Member State - to impose tougher penalties on companies that fail to comply.

The GDPR applies to EU organisations that process personal data of EU citizens, as well as non-EU organisations that offer products or services to EU citizens or monitor their behaviour.

Key definitions

- Personal data is "any information relating to an identified or identifiable natural person ('data subject')". This includes online identifiers such as IP addresses and cookies.
- Data subjects are natural persons "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier".
- The controller is "the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data". The controller is responsible for ensuring that its data processing complies with the requirements of the GDPR, even if it is carried out by an intermediary.
- A data processor is "a person, public authority, agency or other body which processes personal data on behalf of the controller".

GDPR Principles

Article 5 of the GDPR sets out seven important principles that must be respected when processing personal data and that are at the heart of the Regulation. They are as follows:

I. Lawfulness, fairness and transparency: personal data must be processed 'lawfully', i.e., it must meet at least one of the legitimate bases of the GDPR and not violate other laws. It must also be handled 'fairly', without causing undue harm, surprise or deception to data subjects. Finally, they must be handled 'transparently', meaning that processors must explicitly and openly tell data subjects how their data will be used. Privacy notices are a typical method of informing data subjects.

II. Purpose limitation: personal data may only be collected and used for specific purposes, which must be communicated to data subjects from the outset in the interest of transparency. If a processor later wishes to use the data for a different purpose, it must

either do so in accordance with a specific legal requirement or function, or obtain explicit permission.

III. Data minimisation: in order to limit the amount of data processed, processors should ensure that the data is sufficient to achieve the stated purposes and clearly relates to them. Processors should also not process more data than it is necessary to achieve these purposes.

IV. Accuracy: processors must ensure that the data is accurate and not misleading. They must also keep the data up to date if this is necessary to fulfil the purposes for which it is processed. If errors are discovered in the data - e.g., because a data subject has exercised their right to rectification - these must be corrected (or the data deleted) as soon as possible.

V. Storage limitation: personal data should only be kept for as long as is necessary to achieve the stated purpose(s). In addition, data should be evaluated regularly and deleted when no longer needed.

VI. Confidentiality and integrity: the "necessary technical or organisational means" must be used to ensure data security. This requires a risk assessment and the implementation of appropriate procedures as a result.

VII. Accountability: data controllers must be able to demonstrate that they comply with the other six standards of the accountability principle.

Lawful bases for processing

To process data lawfully, organisations must have at least a 'lawful basis' for processing. Article 6(1) of the GDPR lists six legal bases (consent, performance of a contract, legitimate interest, vital interest, legal requirement and public interest). However, if no other legal basis applies to a particular processing activity, processors must rely on the consent of the data subject. Consent serves as the legal basis for processing personal data in the context of the INTERLINK project.

Article 7 of the GDPR imposes strict requirements on consent. Consent must meet the following criteria to be valid under the Regulation:

- Informed - it must be very clear why consent is being sought and what the data subjects are consenting to.
- It must be given through an affirmative opt-in process - no ticked boxes or other approaches that assume consent.
- Specific and granular - separate consent is required for different things.
- Consent must be freely given - it must be a genuine choice and refusal to give consent must not have an adverse effect on the individual.

Certain categories of personal data are classified as 'sensitive' data under Article 9; if compromised, they may pose a greater risk to the rights and freedoms of individuals than non-sensitive data such as names and addresses. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are considered special categories of data under Article 9(1).The GDPR prohibits organisations from processing such data unless they can rely on a sufficient legal basis and at least one of the ten exclusions listed

in Article 9(2) of the Regulation. This can be done after the data subjects have given their 'explicit consent', but it increases the risks associated with the data processing.

Data subjects' rights

The GDPR grants data subjects the following eight rights:

I. The right to be informed: Article 12 of the GDPR, which is closely linked to the concept of transparency, gives data subjects the right to know what data is being collected about them and how it will be used. This information must be disclosed at the time their data is first collected and is usually included in a privacy notice.

II. The right of access: data subjects have the right of access under Article 15 of the GDPR. This gives them the opportunity to file a 'data subject access request.' This obliges the controller to provide the data subject with a copy of their personal data in an accessible and intelligible format, free of charge, within one month of receiving the request.

III. The right to rectification: Article 16 of the GDPR grants individuals the right to rectification, which includes the correction of inaccurate data or the completion of incomplete data.

IV. The right to erasure: data subjects have the right to erasure (commonly known as the 'right to be forgotten') under Article 17 of the GDPR, which means that processors must stop processing their personal data and destroy it when they exercise this right.

V. The right to restriction of processing: individuals have the right to prohibit processing under Article 18 of the GDPR. If this right is exercised, the processor may shop the personal data but may not process it in any other way.

VI. The right to data portability: according to Article 20 of the GDPR, data subjects have the right to request personal data from controllers in a "structured, commonly used and machine-readable format". This makes it easier for data subjects to re-use their data for other purposes, e.g. by transferring it to another controller.

VII. The right to object: data subjects have the right to object to the processing of personal data in accordance with Article 21 of the GDPR. If a data subject objects, they must explain why they are objecting. The processor must then decide whether the objection outweighs the grounds for processing. Within one month of receiving the objection, the data subject must be informed of the processor's decision, together with a statement of reasons and information on how to lodge a complaint.

VIII. Rights in relation to automated decision-making, including profiling: Article 22 of the GDPR defines the rights of data subjects in relation to automated decision-making, i.e., decisions taken entirely by automated methods without the intervention of humans. An example of this is profiling, where automated data processing is used to evaluate certain aspects of a data subject.

2.1.2 Requirements for INTERLINK

Personal data are processed in the context of INTERLINK, in particular the use case data used to monitor the performance of the project. This data therefore falls within the scope of the GDPR. The above principles must be respected in any processing activity and partners must ensure that data subjects have access to the rights afforded to them under the GDPR.

Key recommendations :

- Obtaining valid consent for each processing activity in accordance with the principle of lawfulness. To ensure that consent is informed, explicit, specific and voluntary, information sheets and consent forms containing all the necessary information must be used.
- The processing of sensitive data shall be avoided unless strictly necessary to achieve the purposes of the project. If necessary, prior consultations with the legal WP and specific information sheets shall be used.
- Adhering to the principles of purpose limitation and data minimisation by ensuring that all personal data collected have a clearly defined purpose and are necessary to achieve that purpose.
- Implementing appropriate security measures for the storage of personal data.
- Ensuring that participants are made aware of their rights under the GDPR and take appropriate action if they wish to exercise them.

2.1.3 Implementation of the requirements

Key implementation measures :

- INTERLINK provides the consortium partners with a template for an information sheet and a consent form. Those documents have been reviewed by the Ethical and Advisory board as part of version 2.0 of the Data Management Plan (hereafter DMP, D6.2), and have also been presented in Deliverable D.5. However, several partners rely on their own information sheets and consent forms. Those documents have also been reviewed in the process of producing DMP version 2.0. Information sheets and consent forms have been used throughout their project and their usage is continuously monitored and will be presented in the final version of the DMP (Deliverable D6.3), due at the end of the project.
- Even though the use of sensitive personal data has been restricted to a minimum, it has been necessary for the correct implementation of the project to rely on the processing of health-data and immigration related data, both of which are considered sensitive. Processing of those particular data are done in compliance with GDPR requirements – notably, partners rely on explicit consent when processing those data.
- All personal data processed throughout the course of the INTERLINK project respect the principles of data minimization, data limitation and purpose limitation.
- INTERLINK's personal data are processed and stored following appropriate security measures as requested by internal procedures for each INTERLINK partners.
- Information sheets, whether provided by the INTERLINK project or by each partner specifically, inform participants and users alike of their GDPR rights. Furthermore, WP 6 (UCLouvain) has been designated as a main contact point for data subjects requests.

2.2 Public Sector Information Directive ('Open Data Directive')

2.2.1 Summary

The Open Data Directive was adopted in June 2019 as a revision of the 2003 Public Sector Information Directive and had to be transposed into national law in all member states by 16 July 2021. The Directive aims to make public data more commercially usable. It formulates the principle that public sector information held by public bodies, as well as publicly funded research data, should be made reusable by default and free of charge (or should not cost more than the marginal cost of providing the data). However, the Directive excludes data in which third parties hold intellectual property rights, data that is kept closed for commercial or statistical reasons, and personal data.

Compared to its predecessor, the Open Data Directive has a much wider scope of application. It covers data from public institutions (such as libraries, museums, and archives) but also from public companies in areas such as water, electricity, public transport and logistics. The Directive also contains changes to the pricing for obtaining data, new rules for high value and dynamic data, and stricter laws on exclusive contracts.

Concerning exclusive contracts, the Directive states that exclusive rights to data may not be granted in agreements between public bodies and third parties. Agreements that aim to restrict access to data to persons other than the third parties involved in the agreement, or where this is foreseeable, must be made public under the new Directive.

In addition, the new Directive contains two new concepts: high-value data and dynamic data. As far as high-value data is concerned, the Directive requires that it be made easily accessible. To determine whether data is valuable, one should assess its potential to provide socioeconomic or environmental benefits, its ability to benefit a large number of users and the extent to which it can contribute to income generation.

Dynamic data is the second concept. According to the Directive, these data include environmental data, traffic data, satellite data, meteorological data and data generated by sensors, whose economic value is determined by the availability and frequent updating of the content. This dynamic data must be made available for re-use by public sector bodies as soon as possible after it is collected via APIs and, where appropriate, mass downloads.

2.2.2 Requirements for INTERLINK

The Open Data Directive applies to public bodies, public enterprises and research institutions. Universities may also be covered by the Directive, depending on their legal status (as a public body, public undertaking or private sector entity) and their activities (in particular, whether they are considered research institutions). Therefore, most of the partners of INTERLINK (with the exception of Cloud'N'Sci Ltd) fall under the scope of the Directive.

According to the Directive, access to data can be requested by companies, other public bodies or public companies, researchers and citizens. In general, the Directive covers all publicly available public sector information, such as geographical, cadastral, statistical or legal data

managed by public bodies and some public undertakings, as well as publicly funded research data. It applies to all types of documents containing such data, including text documents, databases, audio files and film fragments.

However, a few cases are excluded from the application of the Directive. Most importantly, the Directive does not apply to personal data. Therefore, INTERLINK use case data is not affected by the Directive. It is not envisaged that INTERLINK will generate either high-value data or dynamic data.

Key recommandations

- INTERLINK partners that are considered public sector bodies must be prepared to respond to requests from third parties for re-use (although universities are not obliged to do so under Article 4(6)(b)).
- The data from INTERLINK for which re-use requests can be made under the Directive is mainly research data.
- Re-use of documents must be free of charge (only the recovery of marginal costs incurred is allowed).
- The Directive is expected to have only a minor impact on the project, as the resulting data sharing requirements are less stringent than those imposed under the Horizon 2020 research and innovation framework programme.

2.2.3 Implementation of the requirements

- INTERLINK partners that are considered public sectors bodies follow their own internal procedures regarding requests from third-parties for re-use.
- Most research data produced by the INTERLINK data have been released under open access, allowing for an easy and free possibility for re-use.
- Respect of the requirements set by the EU Horizon 2020 framework involves *de facto* the respect of requirements under the Open Data Directive.

2.3 Rules applicable in the EU research and innovation framework programme (Horizon 2020)

2.3.1 Summary

Regulation (EU) No 1290/2013 sets out the rules for participation in the current Horizon 2020 Framework Programme (2014-2020), including the rules for the use and dissemination of results and thus the requirements applicable to data generated as a result of projects funded under these programmes.

As regards the sharing of research data, the Regulation contains open access clauses, included in the Rules for Participation, which encourage data sharing without making it mandatory. The RfP allows beneficiaries of H2020 programmes to take into account intellectual property rights and legitimate interests when deciding which data to make available and which to withhold. Beneficiaries may specify in the grant agreement conditions under which open access to these

results should be granted. However, the general principle for access to research data under Horizon 2020 is as follows: "as open as possible, as closed as necessary".

However, open access to peer-reviewed publications is mandatory. All peer-reviewed publications of a project must be made freely and immediately available via a repository; open access embargoes will no longer be tolerated.

2.3.2 Requirements for INTERLINK

- All peer-reviewed publications of the INTERLINK project must be made freely available via a repository.
- The research data generated in the project should follow the principle of "as open as possible, as closed as necessary." They should be open by default, but IP rights and other legitimate interests may be considered to withhold certain data.

2.3.3 Implementation of the recommandation

Current research results have been published under open access licences. The diffusion of research output will be realized at the end of the project after making sure that any personal data is either anonymized or deleted.

2.4 The Digital Services Act

Once INTERLINK will be released to the public, it will be subject to obligations related to information society services and online platforms as requested by EU law. This has prompted careful legal investigations regarding which EU regulations should be considered regarding the INTERLINK project.

At the current moment, we have identified the Digital Services Act (Regulation 2022/2065) as the principal regulatory framework for INTERLINK as a platform. Its actual application to the INTERLINK platform will however depend on

The Digital Services Act (hereafter, DSA) is part of the EU strategy for the Digital Market and aims at providing online users with a safer Internet where they are sure their fundamental rights, such as freedom of expression, will be respected. The DSA follows a tiered-structure approach for obligations on information society services: the more control a service act on the content it provides, the more obligations it has to follow.

2.4.1 Definitions

As stated above, the DSA defines the following actors, all of which are subject to a cumulative set of obligations – article 1, DSA:

(a) 'information society service' means a 'service' as defined in Article 1(1), point (b), of Directive (EU) 2015/1535

(g) 'intermediary service' means one of the following information society services:

(i) a ‘mere conduit’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

(ii) a ‘caching’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

(iii) a ‘hosting’ service, consisting of the storage of information provided by, and at the request of, a recipient of the service;

(iv) ‘online platform’ means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.

Following our investigation, we believe that a released version of the INTERLINK platform would fall under the definition of an “online platform” under the DSA. The DSA also includes a category for Very Large Online Platforms (VLOPs), which accumulates over 45 million of active users at EU level – art. 33 DSA. As those numbers are currently not within reach for INTERLINK in the near future, we did not review the specific obligations relative to the VLOPs in this document.

Furthermore, at the current stage of the project and given the relative outcome of the project’s exploitation, INTERLINK will possibly fall under the definition of micro- or small enterprise (SME) as defined by EU COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises – article 2:

1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.

2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

3. Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

Therefore, obligations that might have been of relevance will not apply and were therefore not further analysed in this document. This particular situation shall be subject to constant monitoring.

2.4.2 Obligations concerning INTERLINK as on online platform

a. Transparency Obligations – art. 15 and 24 DSA

Article 15 and 24 of the DSA requires online platforms to provide yearly reports containing a series of information. However, article 15, 3. and article 19 of the DSA exempts SMEs from those transparency requirements, with the exception of article 24, 3. of the DSA:

Article 24, 3. Providers of online platforms or of online search engines shall communicate to the Digital Services Coordinator of establishment and the Commission, upon their request and without undue delay, the information referred to in paragraph 2, updated to the moment of such request. That Digital Services Coordinator or the Commission may require the provider of the online platform or of the online search engine to provide additional information as regards the calculation referred to in that paragraph, including explanations and substantiation in respect of the data used. That information shall not include personal data.

b. Terms of services – art. 14 DSA

Article 14 of the DSA obliges intermediary services (which includes online platforms) to lay out their terms of services in a manner compliant to the regulation:

Article 14. 1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format.

2. Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions.

3. Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.

4. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter

Regarding article 14, 1., we note that INTERLINK does not plan to rely on algorithmic-decision making.

Regarding article 14, 3., we note that minors shall not predominantly constitute the users of the platform and that the platform will not be primarily directed at them.

c. Notice-and-action mechanism – art. 16 DSA

Article 16 of the DSA imposes online platforms to put in place a notice-and-action mechanism in order for users to notify platforms of any illegal content or content that is contrary to their terms of services.

Article 16 - 1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means. L 277/50 EN Official Journal of the European Union 27.10.2022

2. The mechanisms referred to in paragraph 1 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices. To that end, the providers of hosting services shall take the necessary measures to enable and to facilitate the submission of notices containing all of the following elements:

(a) a sufficiently substantiated explanation of the reasons why the individual or entity alleges the information in question to be illegal content;

(b) a clear indication of the exact electronic location of that information, such as the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content adapted to the type of content and to the specific type of hosting service;

(c) the name and email address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU;

(d) a statement confirming the bona fide belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete.

3. Notices referred to in this Article shall be considered to give rise to actual knowledge or awareness for the purposes of Article 6 in respect of the specific item of information concerned where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination.

4. Where the notice contains the electronic contact information of the individual or entity that submitted it, the provider of hosting services shall, without undue delay, send a confirmation of receipt of the notice to that individual or entity.

5. The provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice relates, providing information on the possibilities for redress in respect of that decision. 6. Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1 and take their decisions in respect of the information to which the notices relate, in a timely, diligent, non-arbitrary and objective manner. Where they use automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph 5.

d. Statement of reasons – art. 17 DSA

1. Providers of hosting services shall provide a clear and specific statement of reasons to any affected recipients of the service for any of the following restrictions imposed on the ground that the information provided by the recipient of the service is illegal content or incompatible with their terms and conditions:

(a) any restrictions of the visibility of specific items of information provided by the recipient of the service, including removal of content, disabling access to content, or demoting content;

(b) suspension, termination or other restriction of monetary payments;

(c) suspension or termination of the provision of the service in whole or in part;

(d) suspension or termination of the recipient of the service's account.

2. Paragraph 1 shall only apply where the relevant electronic contact details are known to the provider. It shall apply at the latest from the date that the restriction is imposed, regardless of why or how it was imposed. Paragraph 1 shall not apply where the information is deceptive high-volume commercial content. 27.10.2022 EN Official Journal of the European Union L 277/51 3. The statement of reasons referred to in paragraph 1 shall at least contain the following information:

(a) information on whether the decision entails either the removal of, the disabling of access to, the demotion of or the restriction of the visibility of the information, or the suspension or termination of monetary payments related to that information, or imposes other measures referred to in paragraph 1 with regard to the information, and, where relevant, the territorial scope of the decision and its duration;

(b) the facts and circumstances relied on in taking the decision, including, where relevant, information on whether the decision was taken pursuant to a notice submitted in accordance with Article 16 or based on voluntary own-initiative investigations and, where strictly necessary, the identity of the notifier;

(c) where applicable, information on the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means;

(d) where the decision concerns allegedly illegal content, a reference to the legal ground relied on and explanations as to why the information is considered to be illegal content on that ground; (e) where the decision is based on the alleged incompatibility of the information with the terms and conditions of the provider of hosting services, a reference to the contractual ground relied on and explanations as to why the information is considered to be incompatible with that ground; (f) clear and user-friendly information on the possibilities for redress available to the recipient of the service in respect of the decision, in particular, where applicable through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress. 4. The information provided by the providers of hosting services in accordance with this Article shall be clear and easily comprehensible and as precise and specific as reasonably possible under the given circumstances. The information shall, in particular, be such as to reasonably allow the recipient of the service concerned to effectively exercise the possibilities for redress referred to in of paragraph 3, point (f).

5. This Article shall not apply to any orders referred to in Article 9. (NB : this concerns removal of content based on a request by the relevant authorities)

e. Notification of suspicions of criminal offences – art. 18 DSA

Under article 18 of the DSA, online platforms have to report to the relevant authorities any suspicion of the use of their services for perpetrating criminal offences involving a threat to the life or safety of a persons or persons.

Article 18 - 1. Where a provider of hosting services becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.

2. Where the provider of hosting services cannot identify with reasonable certainty the Member State concerned, it shall inform the law enforcement authorities of the Member State in which it is established or where its legal representative resides or is established or inform Europol, or both.

For the purpose of this Article, the Member State concerned shall be the Member State in which the offence is suspected to have taken place, to be taking place or to be likely to take place, or the Member State where the suspected offender resides or is located, or the Member State where the victim of the suspected offence resides or is located.

f. Exemption from SMEs – art. 19

Article 19 of the DSA exempts SMEs from supplementary obligations imposed on online platforms. Therefore, they will not be analysed in this document.

2.4.3 Requirements for INTERLINK

The requirements falling upon INTERLINK under the DSA are relatively minimal given it will fall under the EU definition of SMEs. However, it will be important to put in place some technical measures to ensure correct compliance with the DSA. Furthermore, further discussions regarding the dissemination and exploitation of the platform following the end of the project will need to take place to determine which partner shall be responsible for putting those measures in place.

Key recommandations :

- Ensuring that there is a system in place to estimate the number of monthly active users on the platform in the EU;
- Produce and make public terms of use complying with the requirements of the DSA and ensure their proper application;
- Establish a notice-and-action mechanism so that litigious Interlinkers can be notified to the platforms by its users;
- Establish a statement of reason mechanism to inform users when action is taken on their content;
- Establish a monitoring system to prevent the use of the INTERLINK platform to perform criminal offences;
- Monitor the status of the INTERLINK platform as an SME during further dissemination and exploitation phases.

3. National legislation applicable to INTERLINK activities

3.1 Italian legislation

3.1.1 Digital Administration Code

The "Digital Administrative Code" is a collection of rules on a specific subject that summarises and organises the rules written by AgID (Agenzia per l'Italia Digitale - Agency for a Digital Italy) on the digitalisation of public administration in relations with citizens and businesses.

Through the “Simplifications” Decree entered into force in late 2020, an organic intervention was defined and was aimed, among the others, at enhancing the digitalisation of the public administration. The regulatory update, covered various provisions of the Digital Administration Code in order to encourage the spread of public services online, facilitate and simplify access by citizens and businesses, as well as to simplify procedures and improve efficiency.

For instance, the regulatory renewal, provided relevant incentives for using tools such as SPID (Public Digital Identity System) and the electronic identity card itself, facilitating the document renewal procedures. The Decree also introduced the Single Digital Platform for Notifications of Acts and Measures of the Public Administration to citizens and businesses, replacing the use of paper with digital communications.

Finally, an obligation for public administrations was foreseen to develop their systems in a way that enables remote access to employees, in compliance with the Workers' Statute and data security provisions.

3.1.2 Three-Year Plan for IT in the Public Administration (2020-2022)

The “2022-2024 Three-Year Plan for IT in the Public Administration” promotes the digital transformation of the Country and that of the Italian Public Administration.

In particular, the 2022-2024 update is characterised by the increasingly pervasive presence of the National Recovery and Resilience Plan (NRRP), which represents an extraordinary opportunity to accelerate the execution phase of the digital transformation of the Public Administration.

The strategy is aimed at:

- Fostering the development of a digital society, where services put citizens and businesses at the center, through the digitization of the public administration which is the engine of development for the whole country;
- Promoting sustainable development, ethical and inclusive, through innovation and digitization at the service of people, communities and territories, respecting environmental sustainability;
- Contributing to the diffusion of new digital technologies in the Italian productive fabric, encouraging standardization, innovation and experimentation in the field of public services.

The guiding principles of the Plan are:

- Digital & mobile first: public administrations must implement primarily digital services.
- Digital identity only (exclusive access through digital identity): public administrations must exclusively adopt digital identity systems defined by legislation.
- Cloud first (cloud as first option): public administrations, when defining a new project and developing new services, adopt the cloud paradigm first, taking into account the need to prevent the risk of lock-in.
- Inclusive and accessible services that meet the different needs of people and individual territories and are interoperable by design so as to be able to operate in an integrated and uninterrupted way throughout the single market by exposing the appropriate APIs.
- User-centric, data-driven and agile: administrations develop digital services, providing agile methods of continuous improvement, starting from the user experience and based on the continuous measurement of performance and use and making digital public services available cross-border relevant according to the cross-border principle by design.
- Once only: Public Administrations must avoid asking citizens and businesses for information already provided.
- Public data a common good: the information assets of the Public Administration are a fundamental asset for the development of the country and must be valued and made available to citizens and businesses, in an open and interoperable form.
- Open code: Public Administrations must prefer the use of software with open code and, in the case of software developed on their behalf, the source code must be made available.
- Cross-border by design: public administrations must make relevant digital public services available across borders.
- Secure and privacy by design: digital services must be designed and delivered in a secure manner and ensure the protection of personal data.

The update of the Plan was developed with the continuous involvement of an increasingly broader set of Administrations with specific competences in the various fields (Department for Digital Transformation, Ministry of Economy and Finance, Department of Public Function, National Cybersecurity Agency, Istituto Poligrafico e Zecca dello Stato S.p.A, PagoPA S.p.A., Consip S.p.A.), taking into account both the changes that have taken place in the technological and organisational spheres and, above all, the start of the implementation phase of the NRRP.

3.1.3 AgID Guidelines

There is a Regulation for the adoption of Guidelines for the implementation of the Digital Administration Code (DAC). AgID adopts the following types of guidelines pursuant to the DAC, or specific regulatory provisions:

a. “Address” Guidelines: containing general rules whose definition of the detailed aspects is delegated to the individual Administration

b. Guidelines containing technical rules: containing the general rules and the definition of the detailed aspects, in a specific technical Annex, which is an integral part of the guidelines themselves.

The Guidelines are intended for:

- Public Administrations;
- Bodies managing public services;
- Publicly controlled company; private (for the parts of competence)
- Private subjects that provide services to Public Administrations. Some guidelines related to INTERLINK are described in the following sub-sections.

3.1.4 Guidelines on the enhancement of public IT assets

This document represents the guidelines for the enhancement of public information assets for the year 2017 published by AgID.

This paper represents a guideline document which aims to support Public Administrations in the process of enhancing their public information assets, proposing a series of actions that must necessarily be undertaken to implement this process homogeneously on a national scale. On the one hand, the document explores a model and a reference architecture for public sector information, identifying basic standards, formats, vocabularies/ontologies for reference and "core" data, recurrent and independent from application domains, national descriptive metadata profiles; on the other hand, it investigates the organizational and data quality aspects necessary to identify the roles and professional figures of Public Administrations as well as the phases of the processes for the management and publication of quality.

3.1.5 Guidelines on the technical interoperability of Public Administrations and Guidelines on Technologies and standards for the security of interoperability through API of computer systems

Both Guidelines contribute to the definition of the interoperability model of Public Administrations, defined by AgID, in line with the new European Interoperability Framework. The former focus on technologies and their methods of use to ensure the security of digital transactions carried out between and towards Public Administrations that use the application programming interfaces via a computer connection network (hereinafter API). The latter identify the technologies and standards that Public Administrations must take into consideration when creating their IT systems, to allow information and IT coordination of data between central, regional and local administrations. This also allow coordination between Italian services with European public and private entities.

3.1.6 Implications for INTERLINK

The above legislations and guidelines do not contain strict practical requirements for the project. However, they contain indications of general trends that Italian policy makers would like to see implemented and that are compatible with the general direction of INTERLINK.

3.2 Latvian legislation

3.2.1 Digital Transformation Guidelines 2021-2027

Latvia has adopted a set of 'Digital Transformation Guidelines 2021-2027' that centralise previously fragmented digital transformation policies. The goals they highlight in relation to digitalisation, which can be found at INTERLINK goals:

- Open public digital service platforms to businesses to facilitate overall digital transformation.
- To provide open, interoperable, and easily accessible platforms for public digital services for collaboration outside public administration, both at national level and within the EU, by 2027.
- Promoting digital skills of citizens/residents is listed as one of the priority actions.

3.2.2 Service Environment Development Plan 2020-2023

The Cabinet of Ministers approved a medium-term planning document in early 2020 titled "Service Environment Development Plan 2020-2023". It states that the national vision of service delivery is to provide user-centered, proactive services to citizens and businesses that are equally accessible to all by harnessing modern technological capabilities, innovative solutions and collaboration at the national level and across borders. Importantly in the context of INTERLINK, this plan facilitates the unification of services. It states that the government must work closely with municipalities to further develop unified services. Since 2018, work has been underway to standardise service names and short codes, and initially 77 templates for unified municipal services have been published. However, not all municipalities have yet caught up to the same level. Further methodological support is needed to improve the infrastructure for uniform municipal services.

3.2.3 State E-services Regulation

In 2017, the Cabinet of Ministers adopted Regulation No. 402 "State E-Services Regulation", which promotes the further digitalisation of public services. It lists indicators (at least 5000 interactions per year, at least 10% of institutions' service traffic, cost efficiency, improved accessibility, convenience, reduction of administrative burden, optimisation of services, reduction of time and costs, and fair treatment of different groups), one of which is sufficient to prioritise the digitisation of services, which overall has increased the number of public digital services available. It states that user orientation is one of the guiding principles in the development of digital services. This regulation also creates a favourable legal environment for digital services. For example, service owners must try to offer shorter execution times and/or lower fees (if it is a paid service) to facilitate the switch from face-to-face to digital services. In addition, the government is now generally trying to follow the principle of "digital by default" in the provision of services.

3.2.4 Monitoring Framework for State Information Systems Development Projects

Latvia is moving towards centralisation of the digital environment to establish uniform technical and monitoring principles for state digital solutions. In 2021, the Cabinet of Ministers adopted Regulation No. 597 "Monitoring Framework for State Information Systems Development Projects", which sets out principles for the unification of systems. In the future, it will be possible to build the state digital architecture according to common guidelines and to reuse and share parts of different systems. In Latvia, this regulation is called a "digital building authority", which is an unofficial term. This regulation is similar to a building authority that sets the framework for the building blocks of future development projects in the context of digital transformation reforms.

Following Regulation No. 597, amendments to the State Information Systems Law are also planned. Overall, the law will aim to create interoperable systems. Currently, a data management infrastructure is being built to ensure greater interoperability by centrally managing data flows between institutions and services to build the physical infrastructure to implement the once-only principle.

3.2.5 Municipalities Law

The Municipalities Law entered on 1st January 2023. It is designed in a way to enable citizens of local municipalities to participate in local affairs. New introductions include:

1) Formation of citizens' councils – consulting bodies which can be formed even on neighbourhood levels that will participate in questions related to cleanliness, overall development of the physical environment, education affairs, and facilitation of economic activity.
2) Obligation to allocate at least 0.5% of the budget (yearly average income from income and property taxes of last 3 years) should be allocated for citizens' projects as participatory budget.
3) Easier terms for public hearings.
4) Specific provisions allowing collection submissions from citizens (depending on a size of the municipality – 100-2000 signatures needed).
5) Introduction of municipal referendums.

3.2.6 Implications for INTERLINK

Overall, Latvian national policy planning documents, laws, and regulations digital transformation policy aim for less fragmentation and more coordination. The above-mentioned documents do not contain any specific requirements for the project, but indicate strong structural support from Latvian policy makers for the general direction of INTERLINK.

3.3. Spanish legislation

In addition to transposing the General Data Protection Regulation and the Open Data Directive, Spain has adopted the following regulations relevant to the use case of INTERLINK in Zaragoza:

- Law 11/2007 of 22 June 2007 on Citizens' Electronic Access to Public Services.
- Law 15/1999 of 13 December 1999 on the Protection of Personal Data (partially repealed by Law 3/2018).
- Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights.
- At the local level, city councils can develop national regulations and create new regulations applicable to their territory, within the framework of their regulatory powers. In this context, Zaragoza City Council has drafted the Electronic Administration Ordinance which complements the provisions at national level.

3.3.1. Law on Citizen's Electronic Access to Public Services

Law 11/2007 introduced as a new right of citizens the possibility to use electronic means in their relations with public administrations and set a deadline of 2009 to implement the necessary means to do so. In accordance with the provisions of this regulation, the Zaragoza City Council has developed and implemented a complete electronic administrative system, covering both relations with citizens and the processing of procedures within the municipal administration itself. This involved many changes and required a precise and clear definition of the new concepts and rules necessary to replace the traditional means with their electronic equivalent.

It was also necessary to provide citizens with a regulation that sets out in a single text all the rights and obligations as well as the instrumental aspects related to the use of electronic media in their relations with the City Council. Both requirements were met when the Zaragoza City Council adopted the Ordinance on Electronic Administration, which comprehensively regulates electronic administration in the Zaragoza City Council.

3.3.2. Electronic Administration Ordinance

The ordinance provides some clarifications on how the Zaragoza City Council must fully comply with the rights of citizens established in Law 11/2007 and Law 15/1999 on the Protection of Personal Data. These clarifications relate both to fundamental rights and to the effective use of information already held by the City Council and its subsidiary bodies. In addition, the ordinance addresses issues related to fundamental rights in order to provide safeguards and control mechanisms to counteract the opacity of computer systems as they are increasingly used to generate automated decisions.

Law 11/2007 grants legal status to public administration websites and introduces the concept of an electronic government website. The law is complemented in this respect by the ordinance, which defines the objectives of the website and its limits within the catalogue of municipal websites. It aims to lay the foundations for the Zaragoza City Council to promote transparency

and citizen participation in decision-making. Consequently, the electronic website is not limited to the electronic procedures, but is defined as the entire "web space" that contains information directly related to the exercise of municipal competences. It complements the national law by containing provisions that detail the municipality's handling of personal data and that comply with the requirements of the General Data Protection Regulation.

3.3.3. Zaragoza's open government platform

The Open Government and Open Data platform of the Zaragoza City Council is an ideal example of the full implementation of what is set out in the Zaragoza City Council Regulation and in the national legislation described above.

Open Government/Data Zaragoza (https://www.zaragoza.es/sede/portal/datos-abiertos/) is an initiative of the Zaragoza City Council to promote the re-use by citizens, businesses and other organisations of the information published on its website. This is a clear commitment to transparency, increased citizen participation and the possibility of economic growth in different sectors. The platform includes (among many other elements): +150 datasets, +100,000 daily data requests, +250 registered re-users, +40 applications published by re-users.

3.3.4 Implications for INTERLINK

The above-mentioned regulations do not impose any additional specific requirements on INTERLINK, as the requirements set out therein are in line with the requirements of existing EU law. For example, the rules of the Ordinance on Electronic Administration for the processing of personal data by the City Council are aligned with those of the GDPR.

However, the national and local rules and regulations described in the previous sections indicate a strong interest of Spanish policy makers in the digitization of public services and their coproduction, even if they do not contain additional specific requirements. Therefore, they are closely aligned with the objectives of INTERLINK.

4. Intellectual Property Considerations regarding co-delivery

As the aim of INTERLINK is to provide a platform whose goal is to foster collaboration between public and private stakeholders, the questions regarding the intellectual property produced through the use of the INTERLINK platform need to be considered. Given the nature of the platform, we estimate that most (if not all) intellectual property rights applicable to works produced by the platforms will consist of copyright.

Given the broad public that the INTERLINK platform projects to serve, it is neither adequate nor desirable to provide a "one-size-fits all" solution for this particular aspect. Therefore, flexibility should be given to potential users of the platforms in order for them to determine which would be the optimal solution regarding the intellectual property corresponding to the works produced through the use of the INTERLINK platform.

However, INTERLINK relies on the core principles of co-delivery and reuse of results. Therefore, and even though this will not be an obligation for stakeholders using the platforms, INTERLINK will encourage the sharing and re-use of produced works.

To do so, specific Interlinkers will be produced to inform stakeholders on their possibilities and to facilitate their sharing and reuse. Those Interlinkers are to be focused on the production of licensing agreements based on the Creative Commons licensing framework. Those Interlinkers are currently under investigation and will form part of an annex of the final version of the DMP, due at the end of the project.

5. Conclusion

On a practical level, the most important piece of legislation for the INTERLINK project is the General Data Protection Regulation (GDPR), as it sets the rules for collecting the personal data required for the use cases. Care should be taken to obtain valid consent from all participants and to adequately inform them about the collection of personal data and its purposes. The Open Data Directive, while theoretically relevant, is unlikely to have a major impact on the activities of the consortium.

As an H2020 project, INTERLINK adheres to the EU research and innovation framework programme. This means that all peer-reviewed publications of the INTERLINK project must be made freely available via a repository, and the research data generated in the project should follow the principle of "as open as possible, as closed as necessary."

As an online platform, INTERLINK will be subject to several obligations under the Digital Services Act, although those are limited by the status of INTERLINK as an SME. Those obligations will require the implementation of several technical measures before the end of the project and the entry into force of the DSA on January 1 2024.

The Member States where the use cases are located also have relevant laws and guidelines for the digitisation of the public sector. They are closely aligned with the European guidelines in terms of the objectives sought. However, these documents do not contain strict practical requirements for INTERLINK and therefore have little independent influence on the activities of the project.

As the project progresses, upcoming deadlines, such as the expected entry into force of the Data Governance Act in September 2023, need to be closely monitored. An analysis of the final version of the Regulation and its impact on INTERLINK will be added to this document as an addendum prior to its entry into force. Further review on this document will also be available in the final version of the Data Management Plan. As the Data Act is currently not in the process of entering into force before the end of the project, its analysis will not be conducted under INTERLINK.