INTERLINK

WP6 Legal and Ethical Requirements

D6.4 – Initial 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)	Quentin Fontaine (UCL), Alain Strowel (UCL)
Editor(s)	N/A
Reviewers	Taco Brandsen (RU), Danilo Giampiccolo (FBK)
Leading Partner	Alain Strowel (UCL)
Version	V1.0
Deliverable Type	R
Dissemination Level	PU
Date of Delivery	31.12.2021
Submission Date	07.01.2022

VERSION HISTORY

Version	Issue Date	Status	Changes	Contributor
0.1	15/12/2021	Draft		UCL
0.2	31/12/2021	Pre-Final	Section 3.3 on Spanish legislation to be added	UCL
1.0	07/01/2022	Final	Addition of Sec. 3.3 and final revision	ZGZ + UCL

Table of contents

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. The current version of the report was produced in M12 of the project, before the launch of the INTERLINK use cases. It will be updated as the activities of INTERLINK evolve and as the legal framework changes. The final version of the report will be presented in M28.

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 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.

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 6.1) 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 5 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. They 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 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 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.

2.2 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 socio-economic 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 recommendations

- 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.

2.3 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.

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.

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

The "2020-2022 Three-Year Plan for IT in the Public Administration" promotes the digital transformation of the country and that of the Italian 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:

- 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;
- Security and privacy by design: digital services must be designed and delivered securely and guarantee the protection of personal data;
- 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.

The objectives of the Plan are based on the indications emerging from the eGovernment Action Plan 2016-2020 and on the actions foreseen by the eGovernment Declaration of Tallinn (2017-2021), whose indicators measure the level of digitization across the EU and detect the actual presence and use of digital services by citizens and businesses.

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 the PA

Some guidelines related to INTERLINK may be:

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. The document, on the one hand, 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, and on the other 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 the information and IT coordination of data between central, regional and local administrations, as well as between these and the Union systems. European, with the managers of public services and private entities.

3.1.6 Implications for INTERLINK

The above legislations and guidelines do not contain strict practical requirements for the project. They do, however, contain indications of general trends that Italian policy 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 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 set 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 co-production, even if they do not contain additional specific requirements. Therefore, they are closely aligned with the objectives of INTERLINK.

4. 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."

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 2022, need to be closely monitored. An analysis of the final version of the Regulation and its impact on INTERLINK will need to be added to this report. The Data Act, expected in 2022, is also likely to be relevant to the project and will need to be considered.