IRIS

Integrated and Replicable Solutions for Co-Creation in Sustainable Cities

Project Acronym:	IRIS
Project Full Name:	Integrated and Replicable Solutions for Co-Creation in Sustainable Cities
Grant Agreement:	No 774199
Project Duration:	5 years (starting 1 October 2017)

Deliverable 4.3

Data Governance Plan

Work Package:	WP4: City Innovation Platform (CIP)
Task:	T4.3 Data Governance Plan
Lead Beneficiary:	NCA
Due Date:	31 March 2020 (M30)
Submission Date:	20 May 2020 (M32)
Deliverable Status:	Final
Deliverable Style:	Report
Dissemination Level:	PU
File Name:	D4.3_-_Data_ Governance_Plan.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 774199

Authors

Surname	First Name	Beneficiary
Hof	Arjen	CIV
Kiseleva	Anastasiya	VUB
Kruse	Thomas	UTR
Lantto	Kim	GOT
Roux	Stephane	NCA

In case you want any additional information or you want to consult with the authors of this document, please send your inquiries to: irissmartcities@gmail.com.

Reviewers

Surname	First Name	Beneficiary
Kiseleva	Anastasiya	VUB
Gindre	Céline	NCA
Koutli	Maria	CERTH
Holmberg	Lena	IMCG

Version History

Version	Date	Description of the Modifications
0.1	January 7th 2020	First draft created by NCA
0.2	January 20th 2020	Structure of the document and contributors defines
0.3	Feb 7th 2020	1 Introduction by NCA
0.4	Feb 7th 2020	2 Methodology by NCA
0.5	March 4th 2020	5 Use Case 2 by GOT
0.6	March 9th 2020	4 Data Governance Plan by VUB
0.7	April 20th 2020	5 Use Case 1 by UTR 3 IRIS City Innovation platform by CIV
0.8	April 22nd 2020	NCA takes into account the comments made and reviews the document produced by the partners
0.9	April 23rd 2020	VUB takes into account the comments made for the section 4 and updated in accordingly, added references and contributed to the conclusion
1.0	April 30th 2020	Final draft for global Review
1.1	May 12nd 2020	NCA New version based on the reviewers' comments
1.2		Final version to approve by SCO and released to the EU

NCA = Nice Côte d'Azur / UTR = Utrecht / GOT = Gothenburg / CER = Certh / VUB = University of Bruxelles / TYR = TYRENS / CIV = Civity

SCO = Steering Committee

EU = Europe

Disclaimer

This document reflects only the author’s view. Responsibility for the information and views expressed therein lies entirely with the authors. The Innovation and Networks Executive Agency (INEA) and the European Commission are not responsible for any use that may be made of the information it contains.

Executive Summary

The current ambition of the City Innovation Platform (CIP) is to collect, manage and exchange more and more data in the coming years with a growing number of public and private actors. This data, carrying structured or not information, will be created from the internal services of companies or provided by external sources (partners, data providers, data sharing platform, etc.). Each stakeholder could be both supplier and consumer of this data.

The common objective of each stakeholder is to control the added value of their data at their level and to enhance their brand image through their dissemination and promotion to their own organization or to external third parties.

To achieve this, each stakeholder will have to set up a strong traceability on its data throughout its life cycle. Whether created from its organization, routed by standard protocols of an external third party, each data must be identifiable and exploitable in a specific context.

In the same company, for each individual objective to become a common objective, it is imperative to set up a common organization bringing together all the stakeholders around the data. This organization will monitor the management of data both at the functional level and their accessibility at the level of technical platforms.

Similarly, from the vision specific to each stakeholder who will use the data according to these internal mechanisms, it is also necessary to set up cross mechanisms between all the third parties affected in order to manage the data as added value.

Also, through this document, we want to help you to understand the evolution of data within companies, and how to manage it by setting up a shared governance of data in order to configure, transform and exploit it according to each need, by controlling its right of use..

The objective is not to cover all the subjects around the data, but to give orientation on the organization and the processes to set up to guarantee maximum profit.

The document is organized in two main parts:

- a theoretical part that helps you to understand and assess your level of maturity in the concept of Data Governance,
- a practical part to help you implement actions in your approach with 2 use cases.

Table of Contents

Copyright

All brands, trademarks, product names, service names, logos, images, icons cited or displayed herein are the property of their respective owners.

The use of this information does not imply an authorization for the commercial use of unlicensed products by persons wishing to implement the CIP Solution.

All Information about **product** and used in this document are **for identification** and **understanding** purposes only.

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation	Definition
ADE	Application Domain Extension
API	Application Programming Interface.
CIM	City Information Model
CIP	City Innovation Platform
EIP-SSC	European Innovation Partnership on Smart Cities and Communities
EU	European Union
FIWARE	Future Internet-ware
GDPR	General Data Protection Regulation
IoT	Internet of Things
XML	Extensible Mark-up Language
DSA	Data Sharing Agreement
DGP	Data Governance Plan

Table 1 - Abbreviations

List of Terms – Abbreviations and definitions

Abbreviation	Definition
API	A software intermediary that allows for distinct applications or systems to interact with one another.
CIP-component	The following five components of the City Innovation Platform: 1. Data management framework 2. Data market 3. Security and privacy 4. Platform management Proprietary systems connectivity (federated solution)
Data Portal	A software solution (usually a website) that presents a catalogue of searchable and downloadable datasets in a user-friendly and uniform way.
FIWARE	An open software- , API-standard and datamodels framework
Functional requirement	Functional requirements describe the desired end function of a system to assure the design is adequate and meets user expectations. In this document also used as “Design Principles”.

Interoperability	The ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged.
Linked Data	A method of publishing structured data so that it can be interlinked and become more useful through semantic queries, facilitating the sharing of machine-readable data on the web.
Metadata	Data about data
Open data	Data carrying an open license stating it can be freely used, re-used and redistributed by anyone, for any purpose, without limitations.
Open & Agile Smart Cities	Open & Agile Smart Cities (OASC) is a global initiative connecting cities, advocating de facto standards, and sharing best practices.
Reference architecture	A template that offers a common language and support for standards, specifications and patterns, a list of functions and interfaces (APIs) and their interactions with each other.
Role	Responsibility and/or activity of a stakeholder within the CIP
Technical requirement	Technical requirements define what is required to deliver the desired function or behavior from a system to a user’s standards.
TM-Forum	Is a neutral, non-profit member organization.
USEF	This is an international common standard that ensures smart energy technologies and projects are connectable at lowest cost.
XML	This is a mark-up language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Table 2 - Definitions

1. Introduction

1.1.Prerequisites

To fully understand the content of this document and benefit the most of it, it is recommended to first read the following documents:

- D4.1: Document which analyze the existing ICT platforms in order to describe and create a generic and flexible architecture for a common CIP framework.
- D4.2: Document describing the functional aspects of the architecture in accordance with the Functional & Technical requirements “interoperable and open solutions, standards and new business models”.

These documents can also be consulted but since they are more technical, they require mastering a vocabulary and operational experience with Information Technology:

- D4.4: Document translating the use cases of the LH Cities into a technical architecture as a reference for each implementation of the CIP within LH Cities and Follower cities.
- D4.5: Implementation and Integration of core CIP components

1.2. Scope, objectives and expected impact

Task 4.3 of Work Package 4 “City Innovation Platform (CIP)” is described in the IRIS project management plan as “Data Governance Plan”.

The deliverable provides a methodology and practical guide to implement a data Governance Plan in an CIP Architecture.

It provides information applicable to the different parties involved in the IRIS project in accordance with all the common decisions taken to build the current architecture.

This document completes all current documentations describing functional or technical architectures.

1.3. Contributions of partners

The Implementation and Integration of core CIP components is a joint effort between several Cities.

Each of the partners contributed by a set of reflections on the potential and the value of each data collected, in order to consolidate a set of strategic information.

1.4. Relation to other activities

1.4.1. Previous relation

This document is based on the work done upstream and the documents previously delivered.

1.4.2. Joint relationship during the execution of activities

This document includes the work done by the different teams involved in the project.

1.4.3. Next relation

The City Innovation Platform is built on open source technical components and is associated with a set of procedures described in the deliverable D4.5.

Those procedures describe all information about “Configuration / Deployment / Support” to implement a generic API and Data models for a Core CIP components insight a technical infrastructure based on the IRIS environment.

It is the basis for the future activities to guarantee the success of the next tasks for the following work packages:

- WP5: Utrecht LH City demonstration activities.
- WP6: Nice LH City demonstration activities.
- WP7: Gothenburg LH City demonstration activities.

1.5. Structure of the deliverable

Three types of documents were managed during the execution of the task T4.3:

Documentary components

- D4.3 – Data Governance Plan - v1.0.doc

Internal Documents of Nice city for monitoring the progress of the project

- WP4 - T4.3 - MSRyyymmdd – Monthly Status Report.pptx
- WP4 - D4.3 - Data Governance - Action Plan.xls

This deliverable “Document D4.3” is structured as below

Chapter 2 – Methodology: The methodology chapter deals with the definition of the data and its evolution within the company to become a valuable information data. It lists theoretical methodological principles concerning data and its management.

Chapter 3 – IRIS City Innovation platform: In synthetic form, a graphic representation lists the Core components of the CIP architecture, its implementation of generic APIs and data models.

Chapter 4 – CIP Data Governance Plan: This chapter present the foundational principle of the CIP Data Governance Plan in IRIS. This principle is supported by technical, legal, organizational and other measures applied in IRIS about CIP. CIP technical architecture supports different solutions on access, sharing and use of data depending on the role of stakeholder and type of data.

Chapter 5 – Use Cases: This chapter present two use cases implementing the CIP.

Chapter 6 – Conclusions: This chapter presents a summary of this deliverable on the data governance plan which aims to extract the value of the data and increase this value for the different groups of actors involved.

Chapter 7 – References: The chapter provides additional information in the understanding of the document.

2. Methodology

2.1. Introduction

In order to fully understand the objective of data governance and the method of its valuation, it is first necessary to retrace its evolution within companies and the strategic importance it has assumed.

The valorization of the data can only be done by sharing it, in a secure and traceable environment.

In a second part, we will present the contribution of the implementation of a data governance at the level of the whole company, in order to build a global vision of the data and not according to a trade or an application.

Finally, the last part proposes an approach based on the state of the art for the implementation of a data shared from its raw state to a state of value.

2.2. The evolution of the value of the data

2.2.1. From IT to Information Heritage

The information technologies put in place in previous decades were based on a single strategy of automating an existing process to reduce costs. The data were considered only within the limits of their contributions to the proper completion of the treatments.

However, technology is not enough. Today, companies are becoming aware of the knowledge they have or could have internally, by organizing and structuring these above data and transforming it into value-added information.

2.2.2. Data, a valuable resource

Data is now at the heart of the company and the world in which it operates, creating new growth opportunities, but also new challenges.

The importance of data does not need to be demonstrated any longer. Data has become "the precious resource" that everyone must possess in order to manage its informational and socio-economic capital in a context of digital transformation. The performance and quality of the management of this heritage are the cornerstones of all technological projects.

Public or private organizations collect, transform internal and external data into information with values, enriched and adapted to the expectations and needs of each "Users, Citizens, Employees, Decision Makers, Suppliers, Customers, Partners, etc.".

The main objective in the possession of information is its end use, "communication, pooling, budgetary, financial, analysis, forecasts, decision-making for strategic management

This multitude of tasks and interactions between actors explodes the volume of information in different forms through collaborative communication and software tools:

- Messaging, SMS, Social Networks, Blog, Chatbot, Form, etc.
- Document transfer (Dematerialization, Download, etc.)
- Etc.

Together, this creates structured and unstructured data through a network of technical devices (Computers, Mobile, IoT Sensors, etc.) and from different sources.

The increasing exploitation of these new data sources in a competitive logic requires a mastery of its flows and their contents.

It is imperative that the data appear as a source of factual and usable value added. The uninterrupted avalanche of insignificant information will eventually produce the opposite effect.

Acquiring data and using it in a static or non-static logic without looking for its target value, makes it unprofitable to the company.

2.2.3. Data as a common resource

Within the company or organization, an important part of the data lifecycle is the business management's work processes. Whether created by management, transformed, consolidated, communicated or shared, the data belongs to the business branches that process and exploit it functionally.

The Information Systems Division are not intended to replace the business directorates. They are only in charge of proposing technical solutions for projects and their operations (system availability, storage, backup, accessibility, security, availability, reliability, etc.).

With the explosion of data volume and the need for information and communication, the data must open up to the external world in a strong partnership practice approach of sharing, while mastering the image it represents for its owner.

The impact of this proliferation of data on an increasing number of digital channels and people increases the vulnerability of businesses (leaks, data breaches, unwanted and inconsistent data).

The diversity of channels to be managed around the data and the multitude of actors to coordinate in its operation require the definition of an organizational strategy of possession and sharing.

Responsibility for data is not the responsibility of one department or another. Now the data overlap, interconnect with the definition of the concept of co-responsibility for processing between the various stakeholders. In order to ensure its quality and value, all departments of the organization must be jointly owned and managed across the different companies and its partners. The production and supply of data is also extended to external partners, through purchase or exchange contracts. The same is true for a city or a business that hosts a CIP.

The possible exchange of data between different partners, or the connection to shared information sources, requires the establishment of a formal service contract between the stakeholders in order to define all the procedures for exchanging and maintaining them. This contract is defined in an SLA (Service Level Agreement) and QAP (Quality Assurance Plan) and will allow everyone to receive, send, exchange quality and valid data

This strategy requires the implementation of data governance, in order to enhance the value of the data and increase its visibility within and outside the company.

2.2.4. The traceability and confidentiality of the data

The development of the economy is now based on data. The issues attached to controlling this data in terms of strategic positioning and market share are major and directly linked to an essential problem: that of data handling.

In this new organizational strategy focused on its data and traceability (acquisition, circulation, restitution, sharing, etc.), the notions of "data holder" and "responsibility for its exploitation" play a central role in the determination of the entity that has control of the data.

The added value of the data is translated in different ways according to the stakeholders.

It can be functional (provision of a service dedicated to users of his company), lucrative (monetization of his data capital), self-service (download platform), etc.

This multitude of ways to promote data requires the establishment of governance strategies and organizations adapted to the objective sought for its use.

Three types of governance and data organization strategies can be found within a company:

- Internal governance within the company between each department,
- External and contractual governance with partners on marketable data
- Collaborative governance with partners for the exchange of data in a collaborative framework

The possible multitude of governance also requires positioning a global and shared governance of prevention, control and advice to allow the global strategy to be disseminated.

A legal dimension must also be taken into account by the regulatory obligations dictated by "GDPR - General Data Protection Regulations" and the confidentiality of personal data.

Three distinct requirements appear:

- "The confidentiality of personal data».
- "IS security" in which the data are managed in order to protect its from theft, compromise or disclosure.
- chain management and clarity about responsibilities.

For each company or organization, these three requirements raise the question of prioritization in data security.

Indeed, how to assess the criticality of the two requirements on the one hand according to the regulatory risk and on the other hand the essential nature of the data, while continuing to have to manage its activities and the concept of personal data.

2.3. Data governance

2.3.1. Definition

The implementation of data governance helps to define and enforce the principles of data management. It encourages the various business branches to evaluate the benefits that could be brought to them by robust data management. The goal is to build a vision of the data at the enterprise level and not to manage it according to each business or application.

Business Intelligence-oriented data governance will define a set of strong partnership practices (internal/external) by defining between each of the "processes, roles, rules, standards, methods and metrics" around the data. It thus ensures the efficient and efficient use of the information it wishes to acquire, share, archive, erase, protect internally and/or externally.

From this observation, data governance is a cross-cutting operational competence freeing itself from internal mechanical silos within each organization or company by integrating information from external sources into its scope.

This global governance allows us to assess the added value of the data within all companies and its partners involved as provider or consumer of the platform.

This governance and the actions it entails must be established beforehand. The RACI matrix gives a simple and clear vision of who does what in the relations allowing a redundancy of roles or a dilution of responsibilities.

RACI Definition: The RACI matrix is a methodology used for assigning responsibilities and defining roles and responsibilities within a team

- R – ResponsibleHe / She realizes.
- A – Accountable He / She supervises and reports.
- C – Consulted He / She advises.
- I – Informed He / She is informed.

This RACI matrix below is an example of setting up the sharing of responsibilities between the different internal or external partners.

	Business Directions	IT Depart.	Partners
Its purpose in its gross, comprehensive or consolidated operation	R/A		To be define with contractual document
With Its quality by its veracity, its diversity, its specificity	R/A		
Its quantity by volume produced and its freshness according to its periodicity	R/A	I	
Its life cycle	R/A	I	
Its scope and confidentiality with partners	R/A	I	
Enrich and promoting its application heritage with quality data	R/A	I	
The services made available	C	R/A	
Its acquisition or exchange methods	C	R/A	
Its availability	C	R/A	
Its consistency and reliability in its operation	C	R/A	
Its traceability	C	R/A	
Its protection	R/A		

Table 3 - The added value of data within the company and its partners

2.3.2. Place data at the centers of organizations and partners

In order to be able to spread the spirit "Data - A Key Resource" in different companies and its partners, it is necessary both to carry out digital transformation in uses and practices and, above all, to make concrete the vision that puts data at the heart of each stakeholder's strategy.

So that each partner in connection with an organization accepts to communicate their data, or vice versa, it is imperative that all stakeholders are interested. Why entrust information to a Third party or receive it if it does not add value to my Business.

2.3.3. When to set up Data Governance

Relying on data is no longer an option for businesses. Data involves significant challenges to overcome in order to make the most of their value. The problem of data governance becomes a central problem, as soon as the production of data related to internal activities and the collection of information through external flows explodes.

As the points of contact between "Internal Business Organization / Customers / Suppliers / Partners / Governments" increase, the production and volume of data increase exponentially.

Therefore, intelligent use of this data becomes imperative and a project is felt.

Too often, the urgency of having information and the "Time to Market" takes precedence over thinking about mastering and framing data collection and defining its uses.

It is therefore necessary to think about "data governance" ahead of the drafting of the project to build "the vision of data at the enterprise level" and not to manage it according to each business or application.

This reflection upstream of its exploitation will guarantee a better quality of the data in coherence with its use and its desired level of security in the life cycle of the company.

2.3.4. What team to manage my governance

This abrupt change in data and legal constraints has led to the emergence of new skills and professions within companies and organizations.

Each company or organization will have to have teams:

- Trained based on the activities and nature of the organizations
- Sized in coherence to deal with subjects related to the life cycles of the data.
- Individually available for cross-cutting competence to increase maturity and take into account new roles.

These new players must have sufficient leeway to be a player in change and transformation in data management.

They must put in place processes that guarantee the state of the data (reliability, consistency, etc....), its operating process (availability, accessibility, lifespan, etc.), their origins (internal, external, private, open-data public,...), their security (portability, privacy, archiving, safeguarding, ...) their structuring, etc.

They are at the heart of storage decisions (what, where, when, how, periodicity, ...), security put in place, traceability on its operation, etc.

They also ensure that the GDPR and other regulations to which the company is subject are properly complied with.

These responsibility and roles must be entrusted to a multidisciplinary, permanent team that we could call the “Data Governance Council”.

2.4. The approach

Five key considerations need to be taken into account in the development of a data governance strategy:

- A vision of the role of data,
- Management for quality data,
- Compliance with regulations,

- Controlling the life cycle of data,
- Managing the chain of stakeholders.

2.4.1. A vision of the role of data

Each stakeholder is at the core of the data transformation process for a personalized need. At each level of an organization, data has its own information value. This transformation of this value is done by tools based on Business Intelligence.

Each organization must ask itself questions about:

My initial raw data, a static data

- What is its origin and its target for mapping my producers and consumers?
- What is the role and proper use of my data, to make sense of it and increase its value to my organization and my company?
- What are the relationships to be included in the exchange of information (sharing or acquisition) with internal organizations and my external partners?

From static data to information

- The qualification, structuring, and aggregation of several raw data make it possible to transform them into meaningful, perceptible and interpretable information to make sense of it in their context.

From information to knowledge

- Understanding the result of reading and analyzing the information collected, the reconciliation of several information where the use of one's own feedback allows everyone to increase their knowledge of the subject for the benefit of their own organization.

From knowledge to decision

- The proper management of one's knowledge acquisition gives enough values to make decisions in any ever-changing environment.

2.4.2. Data quality management

Not all data is equal. The quality of the data corresponds to the conformity of the data from its raw state to its transformation into knowledge so that it meets the intended uses according to the needs and modus operandi of the users of the company.

This quality is measured by several criteria:

- Unique.
- Identified, described with its validated management rules.
- Controlled in time.
- Complete, Consistent, Consistent, Integrity, Exact.
- Certified regardless of its original nature (format - type).

This management therefore requires the establishment of a data repository that the team and the "Governance Council" must promote within each Business Directorate.

2.4.3. Compliance with regulations

In addition to the internal strategic vision, the implementation of data governance in the company requires taking into account the theme of the regulations on traceability and the modification of the data with the "GDPR" law.

2.4.4. Controlling the life cycle of data

As soon as a technical process of "storage, processing, use, historization or destruction" is carried out, total consistency in the life cycle and use of the data is imperative.

This coherence of the "Transformation of raw data into value for the company" and "Its use within the company" is a key element and requires reflection and vision.

2.5. Good daily practice

Good data-governance will be based on the following three themes:

The operational aspect

- Quality: Ensuring an acceptable level of quality of data to be collected and exploited is a key focus of data governance.
- Repository: Classify according to its use "Trade, Technique, Reference, Personal, ... its location, and its evolution "Raw, Transformed, Consolidated, ... within the Information System and define its management rules.
- High availability: Easily make information available to users through sized and appropriate technical services and means.
- Easy to use data: Respect data standards and optimize it ergonomics, so that all stakeholders throughout the lifecycle of this data easily appropriate its meaning, use and enrichment.
- Data Integrity: Check the consistency of the data both when it is created and in the technical means of its operation.
- Security: Establish appropriate security and confidentiality around the data (employees, users, customers, partners, etc.) applied at all stages of the data's lifecycle and in accordance with the RGPD requirements:
- Traceability: Knowing at all times the use and exploitation of the data to prevent violations,
- Vulnerability: Implementing processes to anonymize the cryptology of sensitive data.

The organizational aspect

- The Governance Council is responsible for establishing the governance framework for data shared and made available to everyone. This framework must be adapted for general and specific to every business stakeholders and users. But in general, it includes strategic planning tasks such as defining data needs, developing data policies and guidelines, and planning for data management projects.
- This framework should also include ongoing monitoring tasks, such as managing and solving data-related problems, tracking data policies, and valuing data assets.
- This data governance board must include members of the business and information systems branches.
- It is also essential that the board has a flexible organizational structure. A good practice is to take a top-down approach. Board management oversees governance, while analysts and data

managers implement policies. Data managers are responsible for providing management with the necessary feedback.

The communication aspect

- The implementation of data governance implies a considerable change in the organization of all stakeholders, especially if they are in a customer / supplier relationship or users of a shared storage and exchange platform. information.
- This is why it is imperative that the board finds a mission that is aligned with the interests of the company and takes into account the strengths of the implementation teams.
- The mission of each data governance program must be clearly communicated and must briefly express the main drivers of the Governance Process within the organization. Likewise, it must be communicated repeatedly and systematically through various channels.

We note that what is needed for good data governance is a matter of technical concerns, a strategic vision and an accompanying plan. It is therefore a work that is conceived over time and which must be gradually infused into the whole company with a process of continuous improvement.

3. IRIS City Innovation Platform

The CIP is an implementation of generic API and Data models for a Core CIP components insight a technical infrastructure based on the IRIS environment.

To facilitate that the CIP offers tools to collect, store and manage data, with appropriate security. The provisioning of data is enabled by offering open standards (like FIWARE) and by providing a one stop shop (Data Market). The marketplace is the place where data providers can expose data to potential consumers. The data-owner has full control what is offered, under which license, for which price and to whom.

The scheme below shows the generic architecture of CIP. The basic concept is that CIP connects supplier and consumers of data

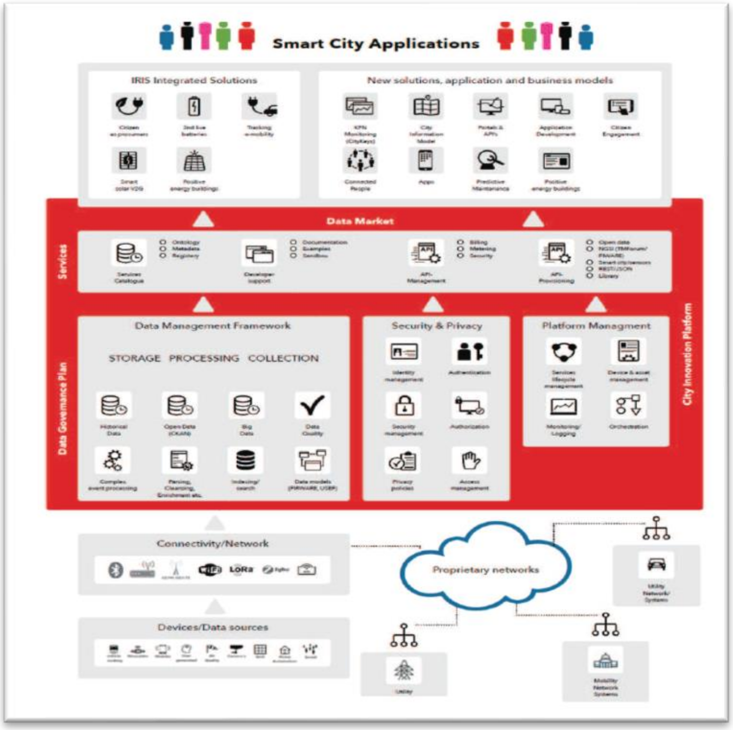

Figure 1 - Generic CIP architecture and the basic concepts to connect supplier and consumers of data

Besides the technical aspects, the success of CIP depends on strong processes and organizational agreements. Therefor CIP combines the best practices from FIWARE and TM Forum. The last one has developed an extensive business framework that is applicable on smart cities too. This framework combines the technical, operational and business governance aspects.

Furthermore, it enables to connect multiple data sources, from municipalities but also data from other stakeholders involved in achieving the IRIS goals.

4. CIP Data Governance Plan

The CIP Data Governance in IRIS is based on the distinction between different types of data collected, processed and generated in the platform and roles of stakeholders involved in its governance. "In smart city projects, a variety of interests come into play: the interests of citizens, authorities, technology vendors, regulators, researchers and lawmakers. These different stakeholders will also have different perspectives on what should happen with the data that are collected and processed in smart city projects, especially when those data are personal."[1]

However, the foundational element in defining the roles of stakeholders and compliance procedures is the type of data. These types are personal and non-personal data. These two types of data are regulated by different laws and by different principles of collection, use and sharing. For example, **personal data** is confidential and its processing is based on the protection of fundamental right of data subject guaranteed by the EU Charter of fundamental rights and specified by the GDPR. Thus, data subject is one of the main actors in collecting and processing his/her personal data. The activities with regard to personal data are limited by principles and rules posed by the GDPR. On the other side, **non-personal data** might be both confidential and non-confidential depending on its commercial value and restrictions of data holder. The main conditions that define the restrictions and limitations with regard to the use of non-personal are defined in agreements between data provider and data user. However, one of the core values of the EU with regard to data (both personal and non-personal) is ensuring free flow of data that allows companies and public administrations to store and process non-personal data wherever they choose in the EU.[2] Thus, the data shall be shared and processed in compliance with agreements' conditions but respecting the core values of the EU.

Another basic principle of the CIP Data Governance Plan in IRIS is compliance with regulations applicable to the use of described types of data and at the same time supporting the value of data as the key element of CIP, as well as its quality, availability and power. This principle is supported by technical, legal, organizational and other measures applied in IRIS with regard to CIP. CIP technical architecture supports different solutions on access, sharing and use of data depending on the role of stakeholder and type of data. For example, CKAN, the open source Data Management System (DMS), allows for storing public and private datasets.[3] Public datasets are open to everyone. Private datasets are only accessible for people with the appropriate rights. Thus, depending on the type of data (personal and non-personal) and type of confidentiality the platform provides the choices supporting compliance measures. Additionally, the Data Market is an online store for different data products and types (open, commercial datasets and information products) from different sources/organizations and aimed at different users. Data types can be mixed and structured in a variety of ways and can be made available as download, API or other arrangements.[4]

[1] VUB Chair. Data Protection on the Ground. Personal data protection in smart cities. Roundtable report. September 2019. Available at: < https://smit.vub.ac.be/wp-content/uploads/2019/09/Report-roundtable-data-protection-in-smart-cities_def.pdf>

[2] EU Policy. Free flow of non-personal data. < https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>

[3] IRIS Deliverable 4.4. Document with technical solution reference architecture for CIP components. P.33.

[4] D4.4. P. 47

The section below describes the compliance measures to be taken as the part of the CIP Data Governance Plan. The measures are described separately with regard to collecting, sharing and use of data in CIP. They are also with regards to personal and non-personal data.

4.1. Data Collection and Generation

The most important step in the governance of both personal and non-personal data in CIP is its collection. CIP is a complex technological system that involves different actors and different types of data. While data is the core component of the system, it is necessary to anticipate its usage in advance, before adding this data to the platform. "Much of the ICT systems cities rely on are third-party services. In many cases, data and application are sold as one proprietary package. This dependency on vendors causes problems for cities when they want to change providers without incurring prohibitively high switching costs or loss of data. Contracts often do not include specific provisions for ownership of the data, access to data, or usage rights."[5] Similar concerns apply to the use of personal data in CIP. Its processing requires compliance with many rules, imposes specific obligations on data controllers and is aimed to ensure respect of data subjects' rights. **Thus, to avoid costs or any disruptions in the platform's functioning caused by change of data provider (or difficulties with the GDPR compliance), at the earliest stage of adding the data to CIP it is crucial to understand the type of data, actors involved in its use, their purposes and anticipated activities with the data.** This section further describes what concerns shall be taken into consideration with regard to collecting personal and non-personal data.

4.1.1. Non-personal data

IRIS CIP Platform will collect non-personal data of different types from different sources, by and from different stakeholders. The datasets might be openly and freely accessible or commercial ones. Thus, the procedures to collect these types of data are different.

For example, when the data is openly and freely accessible, the conditions of its collecting are simplified. However, the simplified conditions do not equal to absence of limitations. One of the examples of **openly and freely accessible** database is the initiative supported by the City of Utrecht. "Utrecht strongly favors collecting and sharing urban data by means of an open ICT urban data platform (utrecht.dataplatform.nl), offering more than 500 data sets and data services for policy development and urban planning processes. These data are also freely accessible for citizens and other stakeholders, for information and for developing data services."[6] Even collecting openly accessible data, data receivers shall always check the terms and conditions of its use because some limitation might be posed there. Specifically, Dataplatform.nl (the large initiative of the Netherlands, Utrecht open data platform is the part of it) has terms and conditions of the data use placed on its website. These terms provide, for example, that specific datasets might be used under the license conditions of data providers. *In IRIS, wherever open data is collected, the terms and conditions of its use will be always checked on its compatibility with the purposes and means to use it in CIP.*

[5] Ine van Zeeland, Jonas Breuer, Rob Heyman, Nils Walravens, Jo Pierson. Policy Brief #25. Connecting the dots – smarter cities work together. 20 May 2019. VUB Chair Data Protection on the ground. Available at: < https://smit.vub.ac.be/wp-content/uploads/2019/05/POLICY-BRIEF-25_20190520.pdf>

[6] D 4.1. P.29

Choosing open and freely usable datasets in CIP is a good option when it is possible considering the aims of data use and its value. Any city platform due to its mere nature involves many users of data (citizens of the city and providers of services), thus, limitations in data usage might prevent from the widest usefulness of data and bear additional operational and other costs (for example, in extending the number of data users). As described above, openness of data is the initiative of many governments and city administrations. Similar to the City of Utrecht Initiative, the Smart Flanders steering approved in 2017 the principles of Open Data Charter. These principles were discussed and co-created by the Flemish Community Commission, 13 centre cities and IMEC. The principles, inter alia, include the following: '*open by default*': data that is captured by, in or about the city is provided as open data for reuse, as the norm; '*comply or explain*': when data is not open, a reasoned explanation should be given as to why it is not; data is made accessible in the context of *transparency* and with the goal of stimulating both *non-commercial and commercial re-use*; *dialogue with all parties collecting data is encouraged* and actively set up, on the initiative of the contact point for open data indicated within the city.[7] All the mentioned are important for governance of data in CIP. However, not all the data might be used openly and freely (and sometimes it is not needed, for example, when the data is necessary for internal infrastructure of for very limited purpose).

When the data is not openly and freely accessible, the terms and conditions of its use are determined in the agreement between data providers (third-party) and data user (CIP's stakeholder) in advance during the contracts' negotiation process. Thus, it is crucial to clearly foresee the purposes, means and entities of the data use in CIP IRIS when it is possible. In case of understanding that due to complexity of the platform and its constant development the changes of the model of the data use might be necessary, the relevant flexible contract terms with possibility of change the contract's conditions during its term will be the solution. However, even with flexible contract, it is crucial to understand before entering the contract what data, how and by whom might be used under the specific agreement and if it is not compatible with IRIS CIP platform, negotiate its change or look for alternatives.

The agreement that specify the terms and conditions of data's use are usually generally identified as 'data sharing agreements' ("**DSA**"). "A DSA can be defined as an agreement between two or more legal entities (or individuals) concerning the sharing of data or information of any kind between these legal entities (or individuals). The notion of 'data sharing agreement' is commonly used to refer to a broad typology of arrangements and documents between two or more organisations or different parts of an organisation."[8] The term DSA herein and after is used for any contract that includes sharing data (including those that have other subject matter but data provision is one of the conditions).

"Depending on the specific needs of the parties, the sharing of data may take different forms, such as for instance reciprocal exchange of data, one or more organisations providing data to one or more third parties, several organisations pooling information and making it available to each other or to third parties, one-off disclosures of data in unexpected or emergency situations, different parts of the same organisation

[7] Smart Flanders. Open Data Charter. 2017. Available at : < https://drive.google.com/file/d/1Xq2-bO8-i0boKC9xqSCTEcU7p2x6Il4g/view >

[8] Julien Debussche, Jasmien César, Benoit Van Asbroeck, Isis De Moortel Big Data&Issues&Opportunities : Data Sharing Agreements. Bird&Bird. April, 2019. Available at : <https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-data-sharing-agreements >

making data available to each other".[9] In IRIS, after defining the source of the data collection (data provider), actors of CIP will cooperate to understand how many entities shall be involved from the side of data user and what are the necessary common terms of the data's use. This information is also important to understand what jurisdiction and laws will be applicable for relevant contract.

"The parties to a DSA are bound to comply with obligations at two levels: mandatory rules arising from the applicable law(s); and contractual terms and conditions specifically set forth and agreed upon by the parties."[10] Applicable contract law rules might concern formal requirements for contract (for example, mandatory written form of the contract), formation, assignment and termination of the contract, liability issues). However, the main substantial terms are negotiated by the parties of relevant agreements. "Within the limits identified above, the parties to a DSA are free to agree on additional terms and conditions applicable to their sharing of data. For instance, the parties may agree on details related to specific obligations connected to the sharing of data, time of disclosure, warranties (or lack of warranties) on the accuracy and completeness of data, obligations of the receiving party to manage the data according to specific rules and to apply certain security measures to protect the data, right of or prohibition to the receiving party to transfer onward/disclose the data to a third party, ownership of the data and intellectual property rights, payment of any consideration for the sharing of data, confidentiality obligations, audit of the receiving party by the disclosing party or by the authorities, warranties on the power to disclose and receive data, duration of the agreement, governing law, and competent court."[11]

To support the principle of free-flow of data in the EU, improve availability of data for business and to lay foundations for a future competitive advantage for European business actors to make the most of data technologies, the European Commission issued the Guidelines on sharing private sector data in the European data economy.[12] The Commission suggests to take into consideration the following in the preparation/negotiation data usage agreements:[13]

Checkpoints for DSA negotiation	Detailed explanation
What data shall be made available?	• **Describe data** which you wish to share as **concretely and precisely** as possible, including the levels of updates to be expected in the future. When interpretative resources that make analytics possible (e.g. methods, models) are shared together with datasets, they should be described.[14] • What **quality levels** can be assured for the data, also over time? Shared data needs to be of good quality, i.e. accurate, reliable and when necessary up-to-date. Ensure that data are not missing, duplicate, unstructured. Specify the source/origin of data and how it was

[9] Ibid

[10] Ibid

[11] Ibid

[12] European Commission. Guidelines on sharing private sector data in the European data economy. Brussels, 25.4.2018 SWD(2018) 125 final. Available at : < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2 >

[13] Ibid

[14] Ibid

	collected/constructed. A mechanism for reporting error in the data may be set up.[15] • Is the data sharing about a **data set** or a **data stream**?[16] • **Ensure compliance with legal obligations** that may prohibit the access or transfer of the data in question to others. Ensure respect of rights that others may have on the data. Verify rights on content represented by the data (intellectual and industrial property rights), if applicable.[17] For this, it is necessary to understand the flow of data after its collecting. • When the shared dataset includes personal data, make sure compliance with the GDPR. For more details, see the relevant sections on collecting, sharing and use of personal data (4.1.2, 4.2.2, 4.3.2).
Who can access and (re-)use the data in question?	• Ensure that the contract defines in a transparent, clear and understandable way **who has a right to access, right to (re-)use, and right to distribute data and under which conditions**. Specify if and how data may be shared for re-use. Be clear when explaining the conditions of contracts for data re-use and sharing. Subcontracting needs also to be considered: either it should be specifically excluded or the conditions under which it is allowed and for what types of data should be specified.[18] • While CIP involves different groups of stakeholders for the use of data, one of the strategies to opt for data providers that are less restrictive in the further use/reuse of data (and always negotiate it during entering the contract). This would enable wide usefulness of data and more potential for the platform. However, it shall be always balanced with the value of the data and potential of its further use/re-use, including the commercial potential.
What can the (re-)user do with the data?	• In the contract negotiations, the (re-)user should be as open and as clear as possible about **how the data is going to be used**, including by parties downstream. This will ensure transparency and increase the trust of the supplier of the data. [19] • Specify the **exact usage that can be made of the data**, including rights on derivatives of the data (analytics).[20]

[15] Ibid

[16] Ibid

[17] Ibid

[18] Ibid

[19] Ibid

[20] Ibid

	• Define **non-disclosure rules** regarding downstream parties[21] (if the data is going to be openly published and accessible, make sure it is stipulated in the contract).
Define the technical means for the data access and/or exchange	This will include: • Frequency of data access and maximum loads; • IT security requirements; • Service levels for support.[22] IRIS stakeholders shall check all the technical requirements for CIP's architecture and check compatibility of data providers' conditions with those requirements. To ensure this compatibility during all lifecycle of CIP's use, the technical requirements shall be stipulated in DSAs as necessary element of data usage and quality.
What data do I need to protect and how do I protect it?	This concern is more important for data providers. However, data users shall be aware of security measures required to use the data for avoiding breach of the contract and its termination. IRIS CIP stakeholders shall verify compatibility of security standards of data providers with security measures applied in CIP. • Ensure that **proper measures to protect data** are in place. These measures should apply to data sharing transactions and to data storage as data can be subject to theft or misuse by organised crime groups and individual hackers. Data can also be released accidentally, for example through human error or because of a technical problem. Data can also be subject to unauthorised access or disclosure or can be lost.[23] • Ensure the protection of trade secrets, sensitive commercial information, licenses, patents, intellectual property rights. Neither party shall aim at retrieving sensitive information from the other side as a result of the data exchanges.[24]
Include rules on liability provisions	Liability might be applicable for supply of erroneous data, disruptions in the data transmission, low quality interpretative work, if shared with datasets, or for destruction/loss or alteration of data (if it is unlawful or accidental) that may potentially cause damages.[25]

[21] Ibid

[22] Ibid

[23] Ibid

[24] Ibid

[25] Ibid

	To make the liability rules work, it is important to define the requirements for data quality and terms of its providing as specified as possible.
Other checkpoints	• Define rights of both parties to perform **audits** on the respect of the mutual obligations.[26] This might be a useful tool to ensure transparency but should be carefully applied for CIP stakeholders due to the amount and differences in participating actors. It is advisable to limit this right to the main data user in case of CIP and/or to cases where the substantial breach of the agreement is suspected. • What is the intended duration of the contract? What rights to terminate the contract? What notice to be given to your partners?[27] • Agree on applicable law and dispute settlement mechanisms.

Table 4 - Consideration in the preparation/negotiation data usage agreements

In summary, CIP's stakeholders will actively cooperate with each other to understand the common needs on the use of datasets in question. Different elements shall be considered when deciding the sources of data collection. The most important element is the value of data and potential for its use/re-use. The other element is conditions of the data collection and use established by data providers. Open and freely accessible data sources is the good source enabling the widest further use of data. When this option is not available, during collecting the data all the necessary terms and conditions will be negotiated with relevant third-party data providers. This will enable avoidance of changing data providers and disruptions in CIP's functioning caused by that.

4.1.2. Personal data

Citizens are one of the main actors and stakeholders in CIP. They are actively engaged in providing and receiving data. With regard to providing data, there may be different means and different sources for that. For example, data can be provided from citizens' vehicles, households, directly added to the platform (such as authorization and/or report issues and give feedback that improves the city). The data received from citizens is not the personal one by default but shall be always evaluated on that matter. The definition of '**personal data'** specified by the GDPR is very broad: 'any information relating to identified or identifiable natural person (data subject).'[28] Thus, data is considered to be personal even if is potentially identifiable to data subject. The GDPR specifies that **identifiable natural person** is anyone who can be identified, *directly or indirectly*, in particular by reference to an identifier such as a name, an identification number, *location data*, an online identifier (e.g. IP addresses) or *to one or more factors specific to the physical,*

[26] Ibid

[27] Ibid

[28] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119 ['*GDPR'*], art. 4

physiological, genetic, mental, economic, cultural or social identity of that natural person.[29] Thus, the data that might be used for identifying not only citizens directly (such as names), but indirectly on its own or with the combination of the other data (such as address/location of citizens' households, identifiers of their vehicles) might be considered as personal data. Additionally, personal data will be collected for providing the services of CIP to citizens through their authorization there.

Another more important issue to consider in governing data in CIP is combining different datasets that at the moment of collecting were not evaluated as those that include personal data. If two datasets separately do not identify any natural persons, there is a possibility that matching data from these datasets might do so. Thus, any combination of datasets shall be always assessed by the entity combining datasets with regard to the ability of combined data to identify natural persons.

As was mentioned in IRIS D4.2 Functional & technical requirements for integrated, interoperable and open solutions, standards and new business models, the CIP will follow Privacy Principles as described in the seven principles of Ann Cavoukian (Cavoukian, 2011): pro-active not reactive, privacy as default setting, PbD, positive sum, security, transparency and user centric. Also, the ISO 29100 standard offers guidance for the functional and technical requirements of the CIP. It mentions consent and choice, purpose, collection limitation, data minimalization, use limitation, accuracy and quality, openness/transparency/notice, individual participation and access, accountability, and security.[30] These principles are in compliance with the principles of protection of personal data specified by the GDPR. Ensuring and respect for all the data protection principles is important at the all the stages of data processing and, most importantly, at the first stage - collection of data while the limits to use the data are basically defined at the stage of its collection.

The principles of data protection and relevant measures to be implemented in CIP are described below:

Principle	Explanation
Lawfulness[31]	Lawfulness means that personal data should be processed under one of the legal grounds specified in article 6 of the GDPR.[32] Legal grounds for collecting and processing of personal data in IRIS CIP are described below in this section.
Fairness[33]	The principle of fair processing governs primarily the relationship between the controller and the data subject.[34] Controllers should notify data subjects and the general public that they will process data in a lawful and transparent manner and

[29] Ibid

[30] D4.2 Functional & technical requirements for integrated, interoperable and open solutions, standards and new business models. P. 40

[31] GDPR, Article 5(1)(a)

[32] GDPR, Art. 6

[33] GDPR, Article 5(1)(a)

[34] European Union Agency for Fundamental Rights and Council of Europe, 2018. Handbook on European data protection law, 2018 edition. < https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf > ["*Handbook on European data protection law*"] P. 118

	must be able to demonstrate the compliance of processing operations with the GDPR. Processing operations must not be performed in secret and data subjects should be aware of potential risks.[35] Citizens is one of the most important groups of CIP's users. Besides compliance with the GDPR, guaranteeing fairness of processing activities is necessary to ensure trust of citizens in the use of the CIP and encourage them to cooperate with the providers of CIP.
Transparency[36]	This principle establishes an obligation for the controller to take any appropriate measure in order to keep the data subjects informed about how their data are being used in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[37] Transparency may refer[38] to the information given to the individual before the processing starts,[39] the information that should be readily accessible to data subjects during the processing,[40] but also to the information given to data subjects following a request of access to their own data.[41] These measures will be implemented in CIP at all the stages of data processing (collecting, use) and by different means: in end-user agreements and privacy policies, informed consent, upon request of data subjects.
Purpose limitation[42]	This principle means that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[43] The purpose of processing data must be defined before processing is started.[44] It is necessary to define the purpose of specific data sets collected from users of CIP or other citizens in advance. Additionally to purposes, it is crucial to understand who will use the data (in case of joint processing, the other purposes might be identified).
Data minimization[45]	The data minimization principle means that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[46]

[35] Ibid

[36] GDPR, Article 5(1)(a)

[37] GDPR, Art. 12

[38] See Handbook on European data protection law, P.120

[39] GDPR, Art. 13 and 14

[40] Article 29 Working Party, Opinion 2/2017 on data processing at work, P. 23. Cross-reference from the Handbook on European data protection law, P. 120

[41] GDPR, Art. 15

[42] Ibid, Art. 5(1)(b)

[43] Ibid

[44] See Handbook on European data protection law, P.122

[45] GDPR, Art. 5 (1)(c)

[46] Ibid

	In CIP, the main aim is to provide the information about city services and activities, not persons. Thus, personal data will be always anonymized when it is possible to keep the usefulness of data.
Accuracy[47]	This principle means that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[48] One of the core components supported by the Open Urban Platform and implemented by CIP is Data Assurance Management.[49] "It will include measures to monitor, validate and — if needed and possible — improve data quality, in aspects like completeness, validity, consistency, timeliness, accuracy, compliance (with respect to regulations or standards), during data recording/entry and/or during further data processing.[50] All the mentioned applies, inter alia, to personal data.
Storage limitation[51]	The storage limitation principle means that personal data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.[52] Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[53]
Integrity and confidentiality[54]	The integrity and confidentiality principle means that that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[55] Similar to ensuring accuracy, one of the core components supported by the Open Urban Platform and implemented by CIP is Data Security Management.[56] It will include, inter alia, managing confidentiality, integrity and availability of data, by means of security policies, processes, people and technologies for user authentication, authorization (functional and data perspective), security zoning, intruder detection etc.[57]

[47] GDPR, Art. 5 (1)(d)

[48] Ibid

[49] D. 4.2. Functional and technical requirements for integrated, interoperable and open solutions standards and new business models. P. 59.

[50] Ibid

[51] GDPR, Art. 5(1)(e)

[52] Ibid

[53] Ibid

[54] GDPR, Art. 5(1)(f)

[55] Ibid

[56] D. 4.2. Functional and technical requirements for integrated, interoperable and open solutions standards and new business models. P. 59.

[57] Ibid

Accountability[58]	This principle means that the controller shall be responsible for and be able to demonstrate compliance with all the previously mentioned principles.

Table 5 - Data protection and relevant measures to be implemented in CIP

As mentioned in the principle of lawfulness, the most important step during collecting personal data is to understand the legal ground for its processing. The legal grounds of processing of personal data that might be appropriate in CIP are the following:[59]

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

To define the appropriate legal basis for processing of personal data in CIP, the purposes of processing should be specified in advance (purposes of all the stakeholders involved, not only those that collect data but also those that receive it from collector), roles of all the stakeholders involved in the processing of data, types of processed personal data and the nature, circumstances, other features of processing should be assessed.

The most relevant ground for the project is consent of data subject. This is because the conditions necessary for the utilisation of the other legal bases are not always likely to exist within the context of a research project. For example, the specific conditions to apply legal ground as performance a task carried out in public interest shall be stipulated in the legislation of Member State to which the controller is subject. Thus, it shall be checked during the real-life use of CIP in specific states with having all the information about data processing. Performance of the contract is the ground that might be applicable at the research phase in case of providing CIP to its users as completed product/service. However, this ground shall be widely used in the real-life application of CIP due to its flexibility and active engagement of citizens in the use of platform. The kind of agreement appropriate for that will be end-user agreement where citizens will read its terms and choose to accept them before the use of CIP. Privacy policy shall describe what data, how and by whom will be used to perform the end-user agreement with citizens.

At the research phase the consent of data subject is likely to be the most important legal base for the processing of personal data (at the implementation phase this legal ground will be used in addition to performance of the contract and performance of a task in public interest). The GDPR provides that **the consent should be**:

- **Freely given.** Consent can be deemed freely given "if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent."[60] The GDPR specifies that "when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the

[58] GDPR, Art. 5(2)

[59] GDPR, art. 6

[60] Article 29 Working Party (2011), Opinion 15/2011 on the notion of consent, WP 187, Brussels, 13 July 2011, P. 12

performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract;"[61]

- **Informed**. Informed consent will usually comprise a precise and easily understandable description of the subject matter requiring consent.[62] The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues , such as the nature of the data processed, purposes of the processing, the recipients of possible and the rights of the data subject;[63]
- **Specific.** For consent to be valid, it must also be specific to the processing purpose, which must be described clearly, and in unambiguous terms. This goes hand-in-hand with the quality of information given about the purpose of the consent. In this context, the reasonable expectations of an average data subject will be relevant.[64]
- **Unambiguous indication of wishes.** Consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.[65] A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.[66]

To comply with the requirements of informed consent (or other legal grounds) and principles of data protection (transparency, fairness, lawfulness, purpose limitation) at the stage of collecting personal data it is important to understand how and by whom it will be processed. In addition, it is crucial to understand if the collected data is necessary for the purposes of CIP and if it might keep its usefulness in case of anonymization. Anonymous information is the information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.[67] In terms of the law, there would be no need to give thought and consideration to the demands of meeting one of the legal bases for the processing of the data68 and to comply with many other requirements, including, inter alia, providing security, privacy by design and by default. In reality this option is far from simple and may be difficult to achieve while often truly anonymous data is of a little use. However, in CIP this option shall be taken into consideration while it often provides an aggregated urban data and the usefulness of data might be kept in this case.

[61] GDPR, Art. 7 (4)

[62] See Handbook on European data protection law, P.146

[63] See Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brussels, 15 February 2007, cross-reference from the Handbook on European data protection law, P.146

[64] See Handbook on European data protection law, P.147

[65] Article 29 Working Party. Guidelines on consent under Regulation 2016/679 17/EN WP259 rev.01. As last Revised and Adopted on 10 April 2018

[66] Ibid

[67] GDPR, Recital 26

[68] Ibid

4.2. Data Sharing and management

4.2.1. Non-personal data

The terms and conditions of sharing non-personal received from external data sources data are basically defined in data sharing agreements. If the shared data has the specific type, it might be protected under additional provisions stipulated under applicable law (for example, data protected as trade secret). Thus, to share non-personal data, it is necessary first to define its type and if any specific laws applicable to it, comply with them. If applicable legislation does not provide regulations on sharing the type of data in questions, then data user shall follow the terms and conditions of data sharing agreement. If the sharing activity is not covered by contract, then is shall be amended for avoidance of its breach and imposing liability. Therefore, all the anticipated sharing activities in CIP shall be stipulated in data sharing agreements during the negotiation phase.

The European Commission in its Guidelines on sharing private sector data in the European data economy described the models of data sharing. The underlying business models of data sharing can differ quite substantially and it strongly depends on the type of data in question and the strategic business interest. They can range from an Open Data approach to exclusive data partnerships with only one party:[69]

- **Open Data approach:** An Open Data approach, whereby the data in question are made available by the data supplier to an in principle open range of (re-)users with as few restrictions as possible and against either no or very limited remuneration, can be chosen when the data supplier has a strong interest in the data re-use. Examples are providers of services that would like to make use of an ecosystem of third-party application developers in order to reach the final customers.[70]
- **Data monetisation on a data marketplace**: Data monetisation or trading can take place through a data marketplace as an intermediary on the basis of bilateral contracts against remuneration. This can be interesting for companies that do not know potential re-users for their data and aim at engaging in one-off data monetisation efforts. This mechanism appears suitable when either (1) there are limited risks of illicit use of the data in question, (2) the data supplier has grounds to trusts the (re-)user, or (3) the data supplier has technical mechanisms to prevent or identify illicit use.[71]
- **Data exchange in a closed platform**: Data exchange may take place in a closed platform, either set up by one core player in a data sharing environment or by an independent intermediary. The data in this case may be supplied against monetary remuneration or against added-value services, provided e.g. inside the platform. This solution allows offering added-value services and thus provides for a more comprehensive solution for more stable data partnerships and allows for more mechanisms of control on the usage made of the data.[72]

[69] European Commission. Guidelines on sharing private sector data in the European data economy. Brussels, 25.4.2018 SWD(2018) 125 final. Available at : < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2 >

[70] Ibid

[71] Ibid

[72] Ibid

Variations and combinations of these models are possible and need to be adapted to each concrete business need. As explained in section 4.1.1, this approach is the most favourable for the IRIS CIP. However, some data (as personal data or proprietary data) might have restrictions in usage, thus, the sharing of data in CIP will have different forms and approaches. When data is received from external sources, the preference shall be given to data providers that support open approach and at the same time ensure value and quality of data. When it is discovered, that the needed sharing option is not specified in the relevant DSA, it is necessary to request the amendment of the contract for avoidance its breach and imposing liability on CIP's stakeholders. For that reason, it is advisable to negotiate flexible terms of contracts' change.

Additionally, the European Commission suggested the following principles of data sharing for B2B sector:[73]

- **Transparency**: The relevant contractual agreements should identify in a transparent and understandable manner (i) the persons or entities that will have access to the data that the product or service generates, the type of such data, and at which level of detail; and (ii) the purposes for using such data;
- **Shared value creation**: The relevant contractual agreements should recognise that, where data is generated as a by-product of using a product or service, several parties have contributed to creating the data;
- **Respect for each other's commercial interests**: The relevant contractual agreements should address the need to protect both the commercial interests and secrets of data holders and data users;
- **Ensure undistorted competition**: The relevant contractual agreements should address the need to ensure undistorted competition when exchanging commercially sensitive data;
- **Minimised data lock-in**: Companies offering a product or service that generates data as a by-product should allow and enable data portability as much as possible. They should also consider, where possible and in line with the characteristics of the market they operate on, offering the same product or service without or with only limited data transfers alongside products or services that include such data transfers.

These principles will be respected and ensured by CIP's stakeholders through active cooperation between them at all the stages of data usage, negotiating terms and conditions of both separated and common data usage, preference to open and free data sources.

4.2.2. Personal data

Sharing personal data is also based on terms and conditions negotiated by data provider and data user. However, the GDPR adds another set of rules for the common use of personal data by different entities. The scope of obligations and responsibilities of the CIP stakeholders with regard to sharing and common processing of personal data will greatly depend on its status under the GDPR – data controller or data processor.

[73] Ibid

The main entity responsible for compliance with data protection rules is the **data controller** while it defines the purposes and means of processing. In other words, the first and foremost role of the concept of controller is to allocate responsibility.[74] While the CIP contemplates the use of data by different stakeholders for different purposes, the concept of joint controllers shall be taken into consideration. "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."[75] They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject, by means of an arrangement between them. The arrangement may designate a contact point for data subjects.[76] Additionally, the arrangement between joint controllers shall duly reflect their respective roles and relationships *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.[77]

Joint controllership of personal data shall be distinguished from its processing by data processor. **The data processor** processes the personal data on behalf of the controller and on the basis of the controller's instructions. "Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may be more general and extended."[78] While data processor acts on behalf of data controller, the lawfulness of the processor's data processing activity is determined by the mandate given by the controller. "A processor that goes beyond its mandate and acquires a relevant role in determining the purposes or the essential means of processing is a (joint) controller rather than a processor."[79]

The controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.[80] Moreover, the controller and processor shall enter into the agreement that specifies the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[81]

Similarly to collecting and sharing of non-personal data, processing activities of personal data shall be defined in advance. When different stakeholders are involved into processing of one or more same CIP datasets or pieces of data, their respective roles must be understood and specified prior to the processing. While most of them serve as technical tools to collect and process data, some others make decision on purposes and means of personal data processing. Depending on that, the roles and responsibilities of the CIP's stakeholders under the GDPR shall be defined and communicated to data subjects. The contracts

[74] Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". 00264/10/EN WP 169. Adopted as of February 16, 2019.

[75] GDPR, art. 26

[76] Ibid

[77] Ibid

[78] Ibid

[79] Ibid

[80] GDPR, Art. 28(1)

[81] GDPR, Art. 28(3)

between CIP's stakeholders shall define purposes of processing of personal data for all the controllers, obligations of all the stakeholders with regard to the GDPR compliance and relevant measures to do so.

4.3. Data Use and Legacy

4.3.1. Non-personal data

As for sharing non-personal data, its usage is defined on the basis of data approach, applicable legislation and terms and conditions of the relevant DSAs. It is necessary to understand if the access to data can be provided to wide audience (for example, citizens) or the relevant measures to ensure its confidentiality shall be taken (and what kind of measures). Again, this shall be defined in advance in relevant DSAs. Additionally, the supply of necessary quality and amount of data shall be ensured during its usage. For that, the updates and support of data provider shall be required and stipulated in DSAs.

4.3.2. Personal data

The use of personal data is basically its processing and is strictly regulated by the GDPR. 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[82]

Thus, processing shall be in full compliance with data protection principles, data controllers' obligations and respect of rights of data subjects. While data protection principles are described in section 4.1.2. , the main provisions related to data subjects' right and obligations of data controllers and described below. CIP's stakeholders will comply with all the mentioned requirements.

Rights of data subjects

Right	Explanation
Right to be informed[83]	The controller shall take appropriate measures to provide to data subject information about data controller (identity, contact detail, contacts of DPO), the purposes of the processing, the recipients of data and other information. It should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[84]
Right of access[85]	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: a) the purpose of processing; b) the categories of personal data concerned; c) the recipients of personal data;

[82] GDPR, art. 4 (2).

[83] GDPR, Art. 12, 13, 14

[84] GDPR, Art. 12

[85] GDPR, Art. 15

	d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e) the existence of the right to request from the controller rectification or erasure of personal data; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source; h) the existence of automated decision-making, including profiling.[86] The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.[87]
Right to rectification[88]	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.[89] These measures also ensure the accuracy principle of data protection.
Right to erasure (‘right to be forgotten’)[90]	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following applies: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based and where is no legal grounds of processing; c) the data subject objects to the processing and there is no other legitimate ground of processing; d) the personal data have been unlawfully processed; e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services.[91]
Right to restriction of processing [92]	The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject;

[86] Ibid

[87] Ibid

[88] GDPR, Art. 16

[89] Ibid

[90] GDPR, Art. 17

[91] Ibid

[92] GDPR, Art. 18

	(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing when the processing is based on public interest or legitimate interest of data controller by pending the verification whether the legitimate grounds of the controller override those of the data subject.[93]
Right to data portability[94]	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on a consent of data subject or performance of the contract and the data processed by automated means.[95]
Right to object[96]	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on public interest or legitimate interest of data controller, including profiling based on those provisions and marketing purposes. The controller shall no longer process the personal data unless some exceptions are applied.[97]
Right to lodge a complaint with a supervisory authority[98]	Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.[99]
Right to an effective judicial remedy against a supervisory authority and to receive compensation[100]	Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered.[101]

Table 6 - Rights of data subjects

[93] Ibid

[94] GDPR, Art. 20

[95] Ibid

[96] GDPR, Art. 21

[97] Ibid

[98] GDPR, Art. 77

[99] Ibid

[100] GDPR, Art. 78 and Art.82

[101] GDPR, Art. 81(2)

Additionally, the GDPR specifies the other obligations of data controllers:

Obligation	Explanation
Demonstration of compliance[102]	The GDPR establishes the general obligation of data controllers to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. The measures shall be implemented taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons; be updated and reviewed where necessary.[103] The examples of the measures to be taken are the implementation of data protection policies; codes of conducts, certification.[104]
Data protection by design and by default[105]	The data protection by design obligation requires data controllers both at the time of the determination of the means for processing and at the time of the processing itself implement appropriate technical and organisational measures, which are designed to comply with data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards.[106] The implementation shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. The example of the measure is pseudonymisation. The data protection by default obligation is the reflection of data minimization and purpose limitation principles. It requires data controllers to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.[107] "That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."[108] In CIP, different measures will be implemented to ensure data protection by default and be design: anonymization and pseudonymisation whenever it is possible, separate technical solutions for personal and non-personal data, different access options depending on the role of the stakeholders (data is not provided to stakeholders that don't need it).

[102] GDPR, Art. 24

[103] GDPR, Art. 24(1)

[104] GDPR, Art. 24(2) and 24 (3)

[105] GDPR, Art. 25

[106] GDPR, Art. 25(1)

[107] GDPR, Art. 25(2)

[108] Ibid

Records of processing activities[109]	The obligation requires data controllers (and processors, if any) to record in writing (including the electronic form) the information about data controller and details about data processing, including, inter alia, the categories of data subjects and categories of data, the purpose of processing.[110] Recording of processing activities is, besides others, is a good tool to demonstrate compliance.
Cooperation with the supervisory authority[111]	"The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks."[112]
Security of processing[113]	The data controller, and data processor (if applicable), shall implement the appropriate technical and organizational measures to ensure a security of data processing.[114] The examples of the measures to be taken are: • the pseudonymisation and encryption of personal data; • the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; • the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; • a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[115] The Handbook on European data protection law suggests the following organizational measures to ensure privacy: • regular provision of information to all employees about data security rules and their obligations under data protection law, especially regarding their confidentiality obligations; • clear distribution of responsibilities and a clear outline of competences in matters of data processing, especially regarding decisions to process personal data and to transmit data to third parties or to data subjects; • use of personal data only according to the instructions of the competent person or according to generally laid down rules; • protection of access to locations and to hard- and software of the controller or processor, including checks on authorisation for access; • ensuring that authorisations to access personal data have been assigned by the competent person and require proper documentation;

[109] GDPR, Art. 30

[110] Ibid

[111] GDPR, Art. 31

[112] Ibid

[113] GDPR, Art. 32

[114] Ibid

[115] GDPR, Art. 32(1)

	• automated protocols on electronic access to personal data and regular checks of such protocols by the internal supervisory desk (therefore requiring all data processing activities to be recorded); • careful documentation for other forms of disclosure than automated access to data so as to demonstrate that no illegal data transmissions have taken place.[116] The measures are defined on the basis of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.[117]
Notification of a personal data breach[118]	The controller shall notify about a personal data beach to the supervisory authority without undue delay and where feasible, not later than 72 hours after having become aware of it.[119] Moreover, data controller shall document the breach and the remedial measures taken. The exception from the notification obligation is the ability of controllers to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons.[120] Moreover, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.[121]
Prior consultation[122]	The controller shall consult the supervisory authority prior to processing where a PDIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.[123]
Stakeholders consultation[124]	Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.[125]

Table 7 - GDPR obligations of data controllers

[116] See Handbook on European data protection law, above fn. 15. P.167

[117] Ibid

[118] GDPR, Art. 33

[119] Ibid

[120] Ibid

[121] GDPR, Art. 34

[122] GDPR, Art. 36

[123] Ibid

[124] GDPR, Art. 35(9)

[125] Ibid

4.4. Summarized approach for the CIP Data Governance Plan

Based on description of handling different types of data during different stages of its use, the following principles of data governance in CIP are specified:

- Differentiating approaches for governance of personal and non-personal data
- Evaluation of data value together conditions of its receiving and further use
- Strong cooperation between CIP's stakeholders at all the stages of data usage
- Anticipating of data usage before the start of the usage
- Compliance with relevant regulations and DSAs

To follow these principles, the following checklist is developed and suggested for CIP's stakeholders to be used through the CIP's data lifecycle. This checklist is based on the previously described guidelines and regulations with respect to collecting, use and sharing of both personal and non-personal data and summarizes the measures to comply with them.

BEFORE COLLECTING:

- Define the type of data (specify what kind of data is included in the dataset in question, answer, if it is possible to identify any natural person with this dataset)
- Define the confidentiality level of the data (personal data is always confidential, non-personal may vary from open data to strictly confidential)
- Define what kind of access will be needed in CIP with regard to the dataset in question (open access/limited access/mixed)
- Define the purposes and benefits/added value of the use of dataset in question
- Define if it is needed to share with other CIP's stakeholders the dataset in question. If yes, specify the relevant stakeholders and their needs with respect to dataset (if they are different from yours, then update the previously defined purposes)
- Define the scope of data providers, as well as their terms and conditions (priorities shall be given to CIP's stakeholders, after that the third-parties' sources shall be checked; if DSA is not publicly available, request it from the data provider, clarify what conditions are non-negotiable for the specific provider)
- Define the data provider that is most applicable for the CIP (required type of access, possibility to share, compatibility with purposes and needs of all the involved CIP stakeholders)
- If none of the data providers is appropriate for the CIP's needs, define what can be negotiated, what can be suggested for data providers in exchange of data provided on the needed conditions (participation in CIP/providing data or services in exchange of received data) or look for alternatives

DURING COLLECTING:

For non-personal data, make sure that the DSA with data provider includes the following:

- Concrete and precise description of data (types, formats, quality requirements (it can be defined, inter alia, trough expected results from the use of data), confidentiality level, necessity for updates, mechanism for reporting errors)

- Description of the procedure to follow to receive the dataset (technical measures necessary for receiving data, security measures, data flow/one (periodical) time provision)
- Description of the procedure to follow to use the dataset (technical and organizational requirements for the unconstrained use of data; security and confidentiality measures to protect the data)
- Specification of all the stakeholders intended to use the data and their purposes (concretely and precisely specify who has a right to access, right to (re-)use, and right to distribute data and under which conditions)
- Specification of access type of data (specify if the data is intended to be made publicly available through CIP or other means and if yes, make sure that the contract includes this provision)
- Specification of cases and procedures to change the contract (when possible, specify the flexibility of data user to change the contract)
- Term of the agreement is as long as possible and the provider does not have unlimited right to unilaterally terminate the contract (it is necessary for avoiding costs related to changing the data provider). However, it is recommended to stipulate in the agreement the right of data user to terminate the contract if the data provider does not comply with its obligations (for example, with regard to the quality of data)

For personal data:

- Define the purpose of data processing
- Check of other CIP's stakeholders or third parties are to be involved in the processing of data. Define their roles, purposes and responsibilities
- Identify what exactly data is needed to achieve the purpose (-s) of processing
- Assess if the purpose (-s) might be achieved by other means without collecting data or with anonymized data
- Define the legal basis for collecting and processing of personal data in question for the identified purposes
- Define the way of notification of data subject about processing activities (how he/she will consent with the data processing activities)
- Define the anticipated risks of data subjects with regard to processing of their data and necessity for DPIA
- Ensure possibility (technical and organizations) to respect all the rights of data subjects, perform all the obligations for data controllers and other GDPR compliance
- Ensure compliance with all the data protection principles

FOR DATA SHARING:

- Define the type of data to be shared (personal/non-personal; confidential/non-confidential, etc.)
- Define the legislation applicable for sharing the identified type of data and rules of that (for example, for personal data, see the section 4.2.2 and other rules of the GDPR)

For non-personal data:

- Define the limitations and procedures of sharing specified in relevant DSA
- If DSA does not allow the planned sharing activity, request amendment of the contract or search for the alternatives

For personal data:

- Define the roles of relevant CIP's stakeholders: joint controllers and/or controller-processor
- Define purposes of data processing for all controllers
- Prepare agreement between joint controllers and/or between controller and processor
- Define in the agreement obligations of all the relevant stakeholders with regards to the GDPR compliance

FOR DATA USE:

- Continuously check the quality and accuracy of data, request data providers for updates and service support when needed, notify about errors in data
- Keep the records of data flows and usage
- Check if the used data is still necessary for the purposes of CIP, and if not, stop using it and delete
- Use appropriate security and confidentiality measures
- Continuously check compliance with rules of applicable legislation

5. Use cases

5.1. Use Case 1 (CIV & UTR)

Use case name	Charging stations
Goals	Improve services for EV to find available parking spots and enforce law when spots are used illegal
Description	The City of Utrecht will add many EV-charging stations to stimulate usage of electric cars. At this moment it is not clear whether a parking spot is really free, because services only look whether a plug is connected to the charging station. It might be possible that a fossil fuel car is occupying the parking spot. To improve this situation sensors are added to the parking spot and the data-stream of the charging station and the parking sensor are combined. If a spot is occupied (noticed by the sensor) and no plug is attached, it will detect an illegal situation.
Technical and organisation Measures	To implement the use case many stakeholders are involved: City of Utrecht: concession holder for EV-charging stations, contract owner for parking sensors, responsible for maintaining public space. • LomboxNet: operator for EV- charging stations • Last Mile Solutions: data provider for EV-charging stations • Communithings: provider of parking sensors • Civity: platform owner To get this use case up and running, the different data streams are connected to the CIP, transformed to the FIWARE-standard and provisioned as standard API. The services are shown in the data market, with appropriate API-management and licenses, to enable delivery of the services to parties that are allowed to use the services.
Legal Measures	No personal data is used This project is a pilot, especially meant to define and arrange the appropriate governance measures. At this moment it is under investigation how the life cycle of data, contract, service levels, licenses, monteization, etc. should be arranged.
Additionnal information	-

5.2. Use Case 2 (GOT)

Use case name	Visualize your city
Goals	Visualize our cities development with BIM data models
Description	The main objective is to give citizens and users an easier way to access/acknowledge projects and means to influence the planning process in order to achieve better and smarter planning through participatory design. Furthermore, the City of Gothenburg and the Urban Transport Administration need to ensure the improvement of city operation performance while improving the citizens’ life. To achieve such objectives, the Urban Transport Administration has to share information and give the citizens a chance to co-create and be a part of the decision-making process. The citizens have to be able to report issues and give feedback that improves the city. By sharing data and information it is expected that the efficiency for the city planners increase. During planning, contracting and building the quality increases by using co-reviewing and collision controls. It may also increase engagement for all parts as it will be easier to be a part of the decisions making process. Before building the planned bridge to Hisingen Island the City officials would like to have feedback from their citizens. They make sure the plans are shown in the City’s relevant application and ask the citizens to give feedback. The citizen wants good mobility in their neighbourhood. They check out the plans in the City's tool for ongoing and future infrastructure constructions to see what the city's plans are. The citizen discovers that the planned bridge to Hisingen island does not have satisfactory bike lanes and comments that. The project administration receives the comment and determines that the comment is relevant and decides to make an amendment in the construction. The project managers and city officials redraw the bike lanes accordingly in their design tool and resubmits the BIM (Building Information Model) file to the CIP. The Citizen can look at the changed plan for the bridge via the City's application that visualizes data coming from the CIP. The project brings the comment into the lessons learned during its retrospective for future constructions to consider. To support the use case, a CIM (City Information Model) data API needs to be developed, where current or new visualization tools easily can access the outcomes of ongoing infrastructure projects in combination with existing geodata and other data. There is also a need for a tool where the BIM providers can submit their BIM-data in a standardized way. You will find more information and Graphics in the D4.4 Document with technical solution reference architecture for CIP components.
Technical and organisation Measures	

Legal Measures	1. Personal data While the ‘vizualize your city’ includes involvement of citizens, their personal data will be processed for that. Conducting authorization in CIP, citizens will provide their consent on processing their data for the purposes of participation in this use case. Only minimum information about participants will be collected (for example, when there is no need to know the real name of the participant, other identifiers might be used (for example, login for authorization). If collecting identifiers is necessary for ensuring quality and source of data, anonymization and pseudonymisation [126] will be used when possible. For example, identifiers might be removed and kept by one stakeholder. The aggregated data without identifiers (for example, reports without the data on citizen provided it) might be shared with other stakeholders and provided for open access. However, removing identifiers does not exclude processing activities from the GDPR compliance. Thus, all the relevant measures will be taken. Personal data will be kept and managed separately from other data in the use case. All the rights of data subjects will be respected and obligations of data controllers will be performed. 2. Non-personal data While the non-personal will be published for the wide audience, the sources of data shall be as open and free as possible. When the data is received from external entities, the relevant DSAs shall stipulate that the data will be made public via CIP and shared with citizens and other CIP’s stakeholders.
Additionnal information	Here we would like to raise a concern of data governance from the traffic department of City of Gothenburg. We are at an impasse regarding publishing this data as open data or shared data. The information owner has decided not to release this dataset based on not knowing the effects of releasing data of this sort to the public. How will this data be used to harm the construction and what kind of safety measures are needed to be considered is uncertain at this moment. We need to find more guidance in the IRIS project and from other partners in Europe on how to solve these kinds of issues. We can for see that this data security issues will increase in the future.

[126] *‘Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*; - art. 4(5) of the GDPR.

6. Conclusions

The goal of this deliverable was to provide the plan to govern data within the frames of City Innovation Platform that enables to extract the value from data and further increase this value for different groups of stakeholders involved. This plan describes different aspects of data governance: a vision of the role of data organizational, operational and communicational aspects of data governing.

One of the core elements of the CIP data governance in IRIS is compliance with applicable laws and regulations. This element is based on distinction of the approaches for different types of data: personal and non-personal types of data.

Personal data is confidential, and its processing is based on the protection of fundamental right of data subject. The activities with regard to personal data are limited by principles and rules posed by the GDPR.

Non-personal data might be both confidential and non-confidential depending on its commercial value and restrictions of data holder. The main conditions that define the restrictions and limitations with regard to the use of non-personal are defined in agreements between data provider and data user.

Taking into consideration the different guidelines and regulation applied to personal and non-personal data governance, the measures to be implemented were suggested and described for different stages of data circle: collection, sharing and usage. Based on that, the common principles to govern data flows in CIP were summarized: differentiating approaches for governance of personal and non-personal data; evaluation of data value together conditions of its receiving and further use; strong cooperation between CIP's stakeholders at all the stages of data usage; anticipating of data usage before the start of the usage; compliance with relevant regulations and DSAs.

Finally, the checklist to govern both personal and non-personal types of data at different stages of data usage (before collecting; during collecting; during sharing and for data usage) for the stakeholders of CIP was developed. The data governance principles were illustrated on the basis of two use cases: "Charging stations" and "Visualize your city".

7. References

7.1. List of links

All links used in the documents are the property of their respective owners. The use of this information does not imply an authorization for the commercial use of unlicensed products by persons wishing to implement this solution.

GENERAL LINKS

IRIS

Co-creating smart and sustainable cities

FIWARE

Fiware Catalogue

Specific LINKS

Legislative sources and non-binding guidelines

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119

Article 29 Working Party, Opinion 2/2017 on data processing at work

Article 29 Working Party (2011), Opinion 15/2011 on the notion of consent, WP 187, Brussels, 13 July 2011

Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brussels, 15 February 2007

Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". 00264/10/EN WP 169. Adopted as of February 16, 2019

European Commission. Guidelines on sharing private sector data in the European data economy. Brussels, 25.4.2018 SWD(2018) 125 final. Available at : < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2 >

Books and articles

European Union Agency for Fundamental Rights and Council of Europe, 2018. Handbook on European data protection law, 2018 edition. < https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf >

EU Policy. Free flow of non-personal data. < https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>

Ine van Zeeland, Jonas Breuer, Rob Heyman, Nils Walravens, Jo Pierson. Policy Brief #25. Connecting the dots – smarter cities work together. 20 May 2019. VUB Chair Data Protection on the ground. Available at: < https://smit.vub.ac.be/wp-content/uploads/2019/05/POLICY-BRIEF-25_20190520.pdf>

Julien Debussche, Jasmien César, Benoit Van Asbroeck, Isis De Moortel Big Data&Issues&Opportunities : Data Sharing Agreements. Bird&Bird. April, 2019. Available at :

<https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-data-sharing-agreements >

Smart Flanders. Open Data Charter. 2017. Available at : < https://drive.google.com/file/d/1Xq2-bO8-i0boKC9xqSCTEcU7p2x6Il4g/view >

VUB Chair. Data Protection on the Ground. Personal data protection in smart cities. Roundtable report. September 2019. Available at: < https://smit.vub.ac.be/wp-content/uploads/2019/09/Report-roundtable-data-protection-in-smart-cities_def.pdf >