Working with data: legal considerations for UDTs

Manuel Portela Charnejovsky (he/him)

Migle Laukyte (she/her)

Universitat Pompeu Fabra

Barcelona
7 November 2025

Profiles

Migle Laukyte

Associate professor in Artificial Intelligence and Law

Manuel Portela Charnejovsky

Research Associate in GeoInformatics

Learning goals

1. **Understand better** the GDPR and its implications for data handling with UDTs
2. **Learn about** the challenges and opportunities related the compliance with the AI Act
3. **Learn how** to implement data governance practices that ensure compliance
4. **Explore strategies** to protect citizens’ privacy and personal data, including data anonymisation techniques and secure data access protocols.

Space for references etc

Working with data: legal considerations for UDTs

Contents

1. Introduction
2. Data Protection
3. AI Act
4. Data sharing and governance
5. Recommendations
6. Conclusions

Use cases

Bratislava

Florence

Glasgow

Kalamata

London

Ostend

Reggio Calabria

Sant Boi de Llobregat

Air Quality

Public space

Mobility

Heritage

Environment

Space for references etc

Which of the following is not a personal data?

A
IP address

B
Mobile app downloads

C
Browsing history

D
All are personal data

Space for references etc

Which of the following is not a personal data?

A
IP address

B
Mobile app downloads

C
Browser history

[✓ **D**
All are personal data]

Which of the following is personal data?

A
Data of your deceased grandmother

B
Data of the taxi company

C
Anonymized data

D
All this data is not personal

Space for references etc

Which of the following is personal data?

A
Data of your deceased grandmother

B
Data of the taxi company

C
Anonimized data

D
All this data is not personal

Which of these AI-based systems involved in safety management could be seen as high risk systems under the AI Act?

A

AI-based system involved in traffic management

B

AI-based system for controlling elevators in a public building

C

GPAI System assisting in the assignment of social benefit

D

All of them are high risk AI systems under the AI Act

Space for references etc

Which of these AI-based systems involved in safety management could be seen as high risk systems under the AI Act?

A
AI-based system involved in traffic management

B
AI-based system for controlling elevators in a public building

C
GPAI System assisting in the assignment of social benefit

D
All of them are high risk AI systems under the AI Act

Space for references etc

Goal: legal aspects of Urban Digital Twins (UDTs)

Addressing the legal considerations of working with Urban Digital Twins (UDTs) is essential for ensuring compliance with data protection and AI regulations and maintaining public trust.

This session will focus on: the legal aspects related to emerging AI regulatory framework (AI Act), compliance and privacy issues, which are critical for the ethical and lawful handling of data within UDTs.

By understanding these legal frameworks, city officials can ensure that their digital twin projects adhere to legal standards, protect citizens’ privacy and personal data, and foster a trustworthy digital environment.

Space for references etc

Working with data: legal considerations for UDTs

Data Protection

Data protection

The **General Data Protection Regulation (GDPR)** lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Balance between:

- Data protection and privacy as fundamental rights
- Free movement: opportunities for companies and organizations to collect, store and manage personal data.

Many UDT projects would **likely not** be covered by the GDPR as they will not directly involve the processing of personal data.

However, personal data is present in the UDT value chain, thus having some implications and posing some compliance and liability risks.

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main scope of application: What is personal data for GDPR purposes?

Processing (Article 4.2 GDPR): 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;

Personal data (Article 4.1 GDPR): any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main scope of application: What is personal data for GDPR purposes?

“Any information”: Identifiers: a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (+ special categories → sensitive data)

“Relating to”

(1) Content: data about a natural person

(2) Purpose: data that is used to assess a natural person

(3) Outcome: data that may have an impact on a natural person

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main scope of application: What is personal data for GDPR purposes?

Reasonable identification (Recital 26 GDPR): “To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used …. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments”.

Re-identification likelihood is the probability in a given dataset of re-identifying an individual. How large is that risk in UDTs?

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main scope of application: What is personal data for GDPR purposes?

Not covered:

- Non-personal data (→ Data Act)
- Data of deceased individuals
- Data of legal persons
- Anonymized data
- Synthetic data
- Aggregated data

Risks with anonymized and aggregated data:

- ❑ Anonymization and aggregation tasks are indeed processing activities
- ❑ Anonymous data ≠ pseudonymised data
- ❑ Re-identification risk

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Are we going to become personal data controllers?

Definition (article 4(7) GDPR):

‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data […].

→ Determination of purposes and means of processing

What is our implication in the elaboration of the datasets used in UDT projects?

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Are we going to become personal data controllers?

Determining who the controller is: Which organization decides?

- To collect personal data in the first place;
- The legal basis for doing so;
- What types of personal data to collect;
- The purpose or purposes for which the data will be processed;
- In relation to which individuals data will be collected;
- If the data will be disclosed, and if so, to whom;
- The information to be offered to data subjects about the processing;
- How to deals with data subjects’ claims; and
- How long the data will be stored.

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Are we going to become personal data controllers?

Joint controllers

Article 26(1) GDPR: “Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information…, by means of an arrangement between them”

- No need to conclude a formal agreement to become joint controllers
- No need that both organizations have access to the personal data at stake

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main obligations under the GDPR.

Principles (article 5 GDPR)

1) Lawfulness, fairness and transparency
2) Purpose limitation
3) Data minimisation
4) Accuracy
5) Storage limitation
6) Integrity and confidentiality
7) Accountability

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main obligations under the GDPR.

Principles (article 5 GDPR): **Lawfulness:** identification of a basis for processing (article 6 GDPR):

- Consent
- Performance of a contract to which the data subject is a party
- Controller's compliance with a legal obligation
- Protection of vital interests of the data subject or a third person
- Processing of data to carry out a task in the public interest
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, subject to balancing of rights

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main obligations under the GDPR.

Principles (article 5 GDPR): **Data minimisation**

The processed personal data has to be:

- Adequate: sufficient to properly fulfil the controller's stated purpose;
- Relevant: it has a rational link to that purpose; and
- Limited to what is necessary: controller does not hold more data than is needed for that purpose.

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main obligations under the GDPR. Compliance with individual rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Data protection

Main obligations under the GDPR. Other accountability obligations for controllers

- Technical and organizational measures aimed at protecting integrity and security
- Selection and supervision of processors and subcontractors
- Auditing and record keeping
- Appointment of DPO
- Data protection Impact Assessment
- Data breach notifications
- International data transfers
- …

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Working with data: legal considerations for UDTs

IA Act

What is AI according to AI Act?

AI system: “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”

Purpose of the AI Act

·The purpose of this Regulation is to

(1) **improve** the functioning of **the internal market** and

(2)**promote** the uptake of **human-centric and trustworthy artificial intelligence (AI)**,

While ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation

Purpose of this act (art. 1.2): This Regulation lays down (I):

(a) harmonised rules for the placing on the market, the putting into service, and the use of AI systems in the Union; **COMERCIALIZATION OF AI IN EU**

(b) prohibitions of certain AI practices; **WHAT KIND OF AI USES ARE PROHIBITED**

(c) specific requirements for high-risk AI systems and obligations for operators of such systems; **HOW TO COMMERCIALIZE HIGH-RISK SYSTEMS, ensuring maximum safety, oversight, control and accountability of those who benefit from it commercially?**

(d) harmonised transparency rules for certain AI systems; **TRANSPARENCY REQUIREMENTS FOR SOME SYSTEMS**

Purpose of this act (art. 1.2): This Regulation lays down (II):

(e) harmonised rules for the placing on the market of general-purpose AI models; **RULES OF GPAI**

(f) rules on market monitoring, market surveillance, governance and enforcement; **RULES ON HOW TO MAKE ALL THESE RULES ENFORCEABLE**

(g) measures to support innovation, with a particular focus on SMEs, including startups **HOW NOT TO DEBILITATE (ALREADY WEAK) POSITION OF SMALL ENTERPRISES THAT CANNOT COMPETE ON THE SAME LEVEL AS BIG (AND ESTABLISHED) COMPANIES**

To whom it applies? And who are you in this list?

1. providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models **in the Union**, irrespective of whether those providers are established or located within the Union or in a third country;

2. deployers—THOSE WHO DEPLOY AI—of AI systems that have their **place of establishment or are located within the Union**;

3. providers and deployers of AI systems that have their place of establishment or are located in a third country, where the **output produced by the AI system is used in the Union**;

4. importers and distributors of AI systems;

5. **product manufacturers** placing on the market or putting into service an AI system **together with their product** and under their own name or trademark;

6. authorised representatives of providers, which are not established in the Union;

7. affected persons that are located in the Union.

How could AI be used in UDT?

1. Traffic management (optimization?)
2. Sustainability
3. Urban planning
4. Predictive maintenance (of infrastructure)
5. Simulation of and preparation for emergency management

Something to bear in mind if we talk about infrastructure and public services: **High-risk AI systems**

High-Risk AI systems in UDT

Annex III of AI Act identifies 8 groups of AI systems which are considered to be high-risk. For the UDTs the most relevant are:

1. **Critical infrastructure:** AI systems that are safety components in the management or operation of critical digital infrastructure, road traffic, supply of water, gas, electricity or heating
2. **Access to and enjoyment of essential private services and essential public services and benefits:** AI systems used:
   a. …
   b. ….
   c. to evaluate and classify **emergency calls** by natural persons o to be used to **dispatch, or to establish priority in the dispatching of, emergency first response** services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems.

However, these systems (in Annex III) are not high-risk if they not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making

What makes a system **low risk** then are the **following conditions, when AI system is intended:**

a) to perform a **narrow procedural task**;
b) to **improve the result** of a previously completed human activity;
c) to **detect decision-making patterns or deviations** from prior decision-making patterns and is **not meant to replace or influence** the previously completed human assessment, without proper human review; or
d) to perform a **preparatory task** to an assessment relevant for the purposes of the use cases listed in Annex III

General Purpose AI (GPAI)

A GPAI is an AI system which is based on a general-purpose AI model, that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.

- GPAI Based on language models: ChatGPT / Gemini
- GPAI based on image generation: Stable Diffusion / SORA

General purpose AI model: means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications.

- GPAI Model based on language: LLaMa / GPT
- GPAI based on image generation: Pico-Banana-400K

GPAI model alone should not be considered a high-risk AI system under the AI Act because models are regulated independently from systems. However, an AI system constructed on top of a normal GPAI model could still be considered high-risk.

GDPR Art. 22 on AMDS

The Article 22 establishes limits for Automated Decision Making-Systems (ADMS).

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

GDPR Art.22, “...[the caseworker or government representative] shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, **at least the right to obtain human intervention on the part of the controller**, to express his or her point of view and to contest the decision.”

https://www.aepd.es/en/press-and-communication/blog/evaluating-human-intervention-in-automated-decisions

Working with data: legal considerations for UDTs

EU Strategy for Data

Which kind of data are not considered part of the high-value datasets and should be made public under the ODD?

A
Geospatial

B
Meteorological

C
Financial

D
Mobility

Space for references etc

Which kind of data are not considered part of the high-value datasets and should be made public under the ODD?

A
Geospatial

B
Meteorological

[✓ **C**
Financial]

D
Mobility

Space for references etc

In which cases, a public sector body can request specific personal data held by private sector under the Data Act ?

A
To respond a public emergency

B
To publish in the open data portal

C
develop or improve products and services

D
carry out scientific research or analytical activities

Space for references etc

In which cases, a public sector body can request specific personal data held by private sector under the Data Act ?

[✓ **A**
To respond a public emergency]

B
To publish in the open data portal

C
develop or improve products and services

D
carry out scientific research or analytical activities

EU Strategy for Data

Open Data Directive (2019)	ADD focuses on making public sector information freely available.
Data Governance Act (2022)	DGA facilitate data sharing by regulating new entities known as data intermediaries and promoting data sharing for altruistic reasons.
Data Act (2024)	DA expands this vision by enabling access to private sector data, including data generated by connected devices and services.
European Health Data Space (2025)	EHDS enhances individuals' access to and control over their personal electronic health data, while also enabling certain data to be reused for public interest, policy support, and scientific research purposes.

Open Data Directive

Regulates the reuse of publicly/available information held by the public sector, based on the general principle that public and publicly funded data should be reusable for commercial or non-commercial purposes.

Excludes protected data (e.g. personal data and commercially confidential data).

What is the relevance for publicly funded UDTs?

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024

Open Data Directive

Reuse. The use, by individuals or legal bodies, of documents held by public-sector bodies or public undertakings.

Public-sector body. The state, regional or local authorities, bodies governed by public law or associations formed by such authorities, or bodies governed by public law.

Public undertaking. Any undertaking over which public-sector bodies have a dominant influence through ownership, financial participation or the rules which govern it; these include those acting as public passenger road or rail transport operators, air carriers and EU shipowners fulfilling public-service obligations.

Dynamic data. Documents in a digital form, subject to frequent or real-time updates due to their volatility or rapid obsolescence; typically data generated by sensors.

Open format. A file format that is platform-independent and made available to the public without any restriction that impedes the reuse of documents.

Open Data Directive

- **Public-sector bodies must process requests for document reuse**, through electronic means where appropriate, making them available within a reasonable time.
- They must also make the necessary arrangements to facilitate the **online search and discovery of** the documents they keep.
- EU Member States must also facilitate the effective reuse of documents, in particular by supplying information on the rights outlined in the directive and by offering assistance and guidance.
- **Dynamic data (sensors, IoT, etc.) must be made available for reuse immediately** on collection via an application programming interface and, where relevant, as a bulk download.
- **Publicly funded research data** can be reused for commercial or non-commercial purposes in cases where they are already made publicly available via institutional or subject-based repositories.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024

Open Data Directive

Documents whose reuse is associated with significant socioeconomic benefits should be made available under particularly friendly reuse conditions. The directive therefore obliged the European Commission to adopt a list of **high-value datasets** which should be made available free of charge, in machine-readable formats, through application programming interfaces and, where relevant, as bulk downloads. The datasets were selected from within six thematic categories set out in Annex I:

- geospatial;
- earth observation and environment;
- meteorological;
- statistics;
- companies and company ownership;
- Mobility.

Full list here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R0138

See Directive summary: https://eur-lex.europa.eu/EN/legal-content/summary/open-data-and-the-reuse-of-public-sector-information.html

Data Act

In addition to establishing measures to boost interoperability in data spaces, data processing services and smart contracts, the new regulation also incorporates an important novelty by regulating data sharing with public entities in exceptional situations:

- the need to obtain data to respond to a public emergency that are not available by alternative means under equivalent conditions
- the impossibility for the public body to dispose of specific data in order to fulfil a task assigned by law and performed in the public interest when all other means at its disposal have been exhausted

In the latter case, the subject of the request may not refer to personal data unless, by the very nature of the request, it is essential to be able to know at some point in time the identity of the data subject. In this case, pseudonymisation will be necessary. Consequently, the guarantees established by data protection regulations must be taken into account.

See Directive summary: https://eur-lex.europa.eu/EN/legal-content/summary/open-data-and-the-reuse-of-public-sector-information.html

Data Act

Limitations

- Unless expressly authorised by the private entity providing the data, **public bodies may not use the data for a purpose other than that for which they were made available.**
- In the field of official statistics or when it is necessary to carry out scientific research or analytical activities which cannot be carried out by the public bodies requesting the data themselves, it is permitted that the data may be transferred to other bodies for the purpose of carrying out such activities. However, the data may only be made available to non-profit or public interest entities such as universities and public research organisations.
- Nor may the data be used to develop or improve products and services related to the entity providing the data, or shared with third parties for such purposes. (Special focus on AI training)
- Finally, the data obtained in application of this regulation cannot be made available to other subjects under the open data and public sector re-use regulation, so its application is expressly excluded.

See Directive summary: https://eur-lex.europa.eu/EN/legal-content/summary/open-data-and-the-reuse-of-public-sector-information.html

Data Governance Act

Chapter II: Re-use of certain categories of protected data held by public sector bodies.

The provisions of Chapter II DGA apply to public sector bodies and only to data that are held by a public sector body and are also protected for one of the following reasons:

- The data are subject to commercial confidentiality (including trade, professional and company secrets, Article 3 (1) (a) DGA) or "statistical confidentiality" (b);
- The data are subject to third-party intellectual property rights (c)) or
- The data are personal data, insofar as these data are not covered by the scope of the Directive on open data and the re-use of public sector information (PSI Directive, (EU) 2019/1024) (d)).

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

Data Governance Act

According to Article 3 (2) DGA, data of public undertakings, public service broadcasters or educational and cultural establishments (recital 12 DGA mentions libraries, archives, museums and theatres as examples) as well as data protected for reasons of public or national security are excluded from the scope of application.

There are also two situations in particular where this Chapter does not apply to publicly held, protected data: (1) data that are protected for reasons of public security, defence or national security, and (2) data that public sector bodies hold for purposes other than the performance of their defined public tasks. Finally, the exchange of data between researchers for non-commercial scientific research purposes is also out of scope of this Chapter.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

Data Governance Act

If a public sector body authorises re-use of data in its possession, it must ensure compliance with the "conditions" set out in Article 5 DGA. These rules are intended to build trust in the use of data and protect any third-party rights: Single information point, non-discriminatory, transparent, proportionate, non-competition, anonymised, etc.

Equal treatment: DGA prohibits granting exclusive rights and contractually or practically restricting data availability to the exclusion of other facilities to the benefit of one individual. An exception should be allowed if the exclusive permission for re-use is in the general interest, is necessary for the provision of a service or product and is impossible by any other means.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

Data Governance Act

The re-use of data held by public sector entities may be made subject to payment of a fee.

Technical requirements for the public sector to ensure confidentiality, security and anonymity.

Pseudo Anonymization is not enough: Article 5 provides also two alternative options: a secure processing environment controlled by a public sector body in case remote access is provided or reuse and processing at the physical premises of a public sector body.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

Data Governance Act

Data altruism organizations (RDAOs) and data intermediary service providers (DISPs) are organizations that enable data sharing from private sectors.

Some organizations included in the definitions of the DGA: Data pools, Data Marketplaces, Data Cooperatives, Data Spaces, Data Trusts, Personal Information Management Systems (PIMS) , etc. (See JRC report)

RDAOs and DISPs must ensure neutrality, transparency and non-discriminatory practices of data sharing.

Data intermediaries will function as neutral third parties that connect individuals and companies with data users.

¿What kind of data would be nice to access that is not currently available?

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868

Recommendations

Before developing the project

- Develop a Data Management Plan and a Data Governance Plan
- Delegate responsibilities to a Data Protection Officer for the project
- Perform Data Protection Impact Assessment
- Perform Security Impact Assessment
- Perform AI impact assessment
- Identify main risks in data sharing
- Define a data governance structure

Collecting the data

- Ensure that contracts reflect responsibilities and data protection measures
- For personal data, include purpose and legal basis into the contracts
- Verify anonymization and non-identification of individuals in case of non-personal data
- Use a data registry to log all data sharing activities

Space for references etc

Recommendations

During the development of the project

- Use a data registry to log all data sharing activities
- Perform rutinary risk assessment and mitigation activities
- Analyse biases on data and algorithms

In deployment of the project

- Comply with AI Act mandates (database registry, reports, etc)
- Adopt voluntary code of conduct
- Perform risk assessments
- Perform an external audit of the system
- Deploy and enable citizen participation mechanisms to co-create and receive feedback (if applicable)
- Train and provide instructions to implement Human Oversight measures
- Support AI Literacy initiatives to increase awareness, skills and knowledge for the users and society

Space for references etc

Questions to warm up the conversation

Data governance:

- Which mechanisms of consent are established?
- How data is collected?
- Who has access to data and who will be the data users?

Data protection and privacy:

- Is data anonymized/pseudo-anonymized?
- What personal identifiers are stored?
- Does dataset contain sensitive information?
- Which methods of perturbation, aggregation, generalizations have been used to anonymize?

Data ownership:

- What are the rights over the data? Over the dataset?
- Are the data controllers and processors correctly identified?

Security:

- Where is the data stored?
- How data is accessed?
- What mechanisms of data sharing are established?
- What type of connections are established between the data?

Space for references etc

Contacts

Migle Laukyte

Associate Professor in Civil Law

migle.laukyte@upf.edu

Manuel Portela Charnejovsky

Research Associate in GeoInformatics

manuel.portela@upf.edu