Working with data: legal considerations for UDTs

Manuel Portela Charnejovsky (he/him)
Antoni Rubí-Puig (he/him)
Universitat Pompeu Fabra

upf. TESI Technology, Society, and Interactions

Barcelona
8 November 2024

Profiles

Antoni Rubí-Puig

Associate Professor in Civil Law

Manuel Portela Charnejovsky

Research Associate in GeoInformatics

Working with data: legal considerations for UDTs

Contents

Goal

Addressing the legal considerations of working with Urban Digital Twins (UDTs) is essential for ensuring compliance with data protection regulations and maintaining public trust. This session will focus on the legal aspects, primarily GDPR 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 foster a trustworthy digital environment.

Space for references etc

Learning goals

- Understanding GDPR and its implications for data handling with digital twins.

- Learning how to implement data governance practices that ensure compliance.

- Explore strategies to protect citizens’ privacy, including data anonymisation techniques and secure data access protocols.

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:

- 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

Open Data and Data Governance

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 o**f 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 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.

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

Use cases

Arezzo
Barcelona
Brno
Brussels
Budapest
Kadikoy
Leuven
Lille
Mariupol
Oslo
Riga
Rome
Tampere
Turku

Resilience

Public space

Mobility

Heritage

Social Benefit

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

Antoni Rubí-Puig

Associate Professor in Civil Law

antoni.rubi-puig@upf.edu

Manuel Portela Charnejovsky

Research Associate in GeoInformatics

manuel.portela@upf.edu