D1.4 Privacy and Ethical LDT Implementation Manual

Best practices to address legal and ethical risks in local digital twins

Project name	BIPED: Building Intelligent Positive Energy Districts
Duration	January 2024 – December 2026
Project ID	101139060
Coordinator	Technical University of Denmark
Type of action	Innovation Action
Call ID	HORIZON-MISS-2023-CIT-01
Website	https://www.bi-ped.eu/
Document name	D1.4 Privacy and Ethical LDT Implementation Manual
Document status	Final
Delivery date	19.12.2025
Dissemination	Public
Authors	Tomáš Pavelka (UTR)

Funded by the European Union

BIPED is funded under the EU Horizon Europe Research and Innovation programme. Grant ID: 101139060. Every effort has been made to ensure the accuracy of information provided in this document, which reflects only the authors' views. The European Commission is not responsible for any use that may be made of the information contained herein. Credits: cover image from Adobe Stock.

Document history

Version	Date	Contributor	Description
0.1	1.9.2024	Tomáš Pavelka (UTR)	First draft
0.2	13.9.2024	Tomáš Pavelka (UTR)	Draft for review
0.3	24.9.2024	Blain Murphy (KPMG) Jiri Bouchal (DRI)	review
0.4	25.9.2024	Vito Michele Pavese (ICTLC / external)	external expert review
1.0	30.9.2024	Tomáš Pavelka (UTR)	Final version
1.1	19.12.2025	Tomáš Pavelka (UTR) Jiri Bouchal (DRI)	Revised version based on the EC Request for revisions (Ref. Ares(2025)10702198 - 04/12/2025) - Added chapter *9. Integration of EC Recommendations on D1.4*

Table of Contents

Executive summary

The Privacy and Ethical LDT Implementation Manual maps privacy and ethical policy and digital twin related elements with reference to the BIPED Data Management Plan (Deliverable D1.3) (DMP) on how the above identified risks are to be managed by the consortium.

First, the deliverable sets out why privacy and ethical issues matter when designing a local digital twin (**LDT**) and what are the key areas of interest. Doing that, and following the principles of the DMP, there is a clear line drawn as regards privacy impact where personal data is concerned (and therefore the compliance is driven by strict GDPR requirements), and where no personal data is involved. In the latter case, other aspects come to the forefront such as security measures, data integrity, and intellectual property (IP) management.

Second, the deliverable is structured to provide best implementation practice for the respective layers of the LDT design, namely

- **Data layer,** which is in itself extraneous to the LDT but the compliance of datasets used is determinative for the privacy and ethics dimension of the LDT as a whole.
- **Back-end**, which is a core of the LDT inner workings and the processing of data and data models that will be happening in the background, especially combinations of datasets and their re-purposing, is again pivotal from the privacy&ethics perspective.
- **Front-end**, the way in which the LDT is displayed and presented, as well as results of any analytics happening on the back-end, are equally pivotal for privacy&ethics perspective.
- **Stakeholder engagement** is also extraneous to the LDT itself but a cornerstone part of the overall project. While the fundamental rules for compliant stakeholder engagement are set out in the DMP, a section of this deliverable is dedicated to provide some summary best practice to conducting ethical surveys.

Third, **ethical audits.** The deliverable proposes targeted ethical audits to be undertaken by the dedicated legal&ethics consortium partner (UTR) at the following stages:

- Data layer - the audit has been already carried out in the form of critically analyzing the dataset requirements for the BIPED project and reflected in specific rules provided by the DMP (Deliverable D1.3 the Data Management Plan). No deeper audit is proposed to check that the data sourcing and use conforms to the license requirements and security measures - this would go beyond what the consortium management can effectively supervise. Compliance with these requirements should be primarily ensured by the consortium partners in line with the DMP and with support of their own DPOs / legal departments. However, partners will discuss whether a targeted audit should be conducted with respect to crowd-sourced soft data, if any.
- Back end - to be carried out once all the required datasets are procured and are being implemented by the technological part of the consortium into the LDT. The main focus of the audit will be different dataset combinations and whether they are duly processed within the LDT backend framework, with focus on certain highly sensitive areas (e.g. soft data from web / social media scraping). This includes a subchapter on lessons learnt from negotiation about data from local district heating provider, which led to data being provided at a level of aggregation that mitigates privacy and ethical risks. (added in version 1.1)
- Front end - to be carried out once user epics are finalized and the LDT is in an advanced stage of development.. The main goal will be to check whether
    a. the user epics correspond with overall ethical aims of the project,
    b. the LDT is contributing to meeting those aims,
    c. evaluate the transparency of the front-end operations, especially with regards to how data sources and models are presented to users.

- Stakeholder engagement: when the consortium conducts engagement with local stakeholders (citizens, communities & local interest group) as opposed to institutional or corporate stakeholders, audit to check how these stakeholders are handled in the engagement process and how the results are presented and incorporated in the LDT and BIPED results overall.

Specific project timeline milestones will be identified for the proposed audits. Under the Proposal, no specific deliverable is expected to result from the targeted ethical audits envisaged by this deliverable, but partners responsible for individual project tasks will be expected to respect audit findings and implement necessary measures.

Annex 1 reproduces a horizontal ethical principles/guide that was developed in context of the H2020 DUET project for data-driven decision making in the cloud. Much of this is reusable in the context of the BIPED LDT.

Annex 2 contains a preliminary privacy&ethics analysis of specific datasets selected for use in BIPED. The main conclusions are mentioned also in the Front-end section.

1. Introduction

The Privacy and Ethical LDT Implementation Manual maps privacy and ethical policy and digital twin related elements with reference to the BIPED Data Management Plan (Deliverable D1.3) (DMP) on how the above identified risks are to be managed by the consortium.

This deliverable seeks to address significant legal and ethical issues which concern the impact of such technology on individuals, stakeholder groups and the society at large.

Several ethical concerns have been already identified, described and mitigated in previous projects that involved creation of digital twin models (for instance, DUET H2020 project). Key lessons are directly transferable to BIPED.

WP1 work streams that are dedicated to these issues have included the DMP, this deliverable, and further work provided by a dedicated legal & ethics partner (UTR) to contribute to compliance of the project and its working with the highest ethical standards.

The deliverable is structured as follows: after high level describing the proposed BIPED digital twin (**LDT**) and setting out the key areas of interest and code of ethics that drive thinking about privacy and ethics, separate chapters provide a deeper dive and recommendations in the following areas concerning an LDT implementation: 4. Data layer, 5. Back-end, 6. Front-end, and 7. Stakeholder engagement. For each of these stages, the deliverable proposes targeted ethical audits (exact timeline milestones to be identified) to maximize impact of these considerations on how the BIPED LDT is implemented and presented.

2. The BIPED Digital Twin

Local digital twin (**LDT**) is a digital representation of a functional territory combining low- and high-velocity data with dynamic models. In other words, LDT is a virtual replica of the city designed to simulate hypothetical interventions, which allows to analyze and compare scenarios for a review of the impacts of each intervention by virtualizing the "trial and error" process, bringing obvious benefits to cities and the urban planning process in particular.[1]

Given the impact on public policies, urban planners, and by extension the LDT, need a broad and diverse view of the city. By combining information, the LDT provides models that help understand urban processes and generate relevant insights.

BIPED deliverable D2.1 (Initial release of the Digital Twin Platform & Architecture) provides further detail on the BIPED digital twin architecture as at M6 of the project. To best tailor the good practice described in this deliverable, it follows the structure of the BIPED LDT and the lifecycle of the data that is powering the digital twin. While the BIPED DMP provides specific rules, this deliverable seeks to present best practices on how to achieve compliance with these rules while maximizing ethical compliance.

- **Data layer** - while it is exogenous to the BIPED system (as BIPED largely relies on data provided by third parties), for compliant ethical implementation it is necessary to implement best practices to sourcing and curating data at the stage before they are fed to the LDT. Most importantly, anonymisation must be completed at this stage.

- **Back-end** - from a privacy perspective, backend mechanics mean further processing of data inputs (using, analyzing, combining, deriving etc.). Design and controls must be in place to ensure legal and ethical compliance.

- **Front-end** - what results and how they are presented is key to ensuring overall ethical and legal compliance. Results provided by LDT are likely to directly influence decision-making by the users. It is useful therefore to provide some general guidance on how such decision making may work and where the legal and ethical considerations come in.

[1] Living-in.EU taxonomy available at https://living-in.eu/taxonomy/term/284

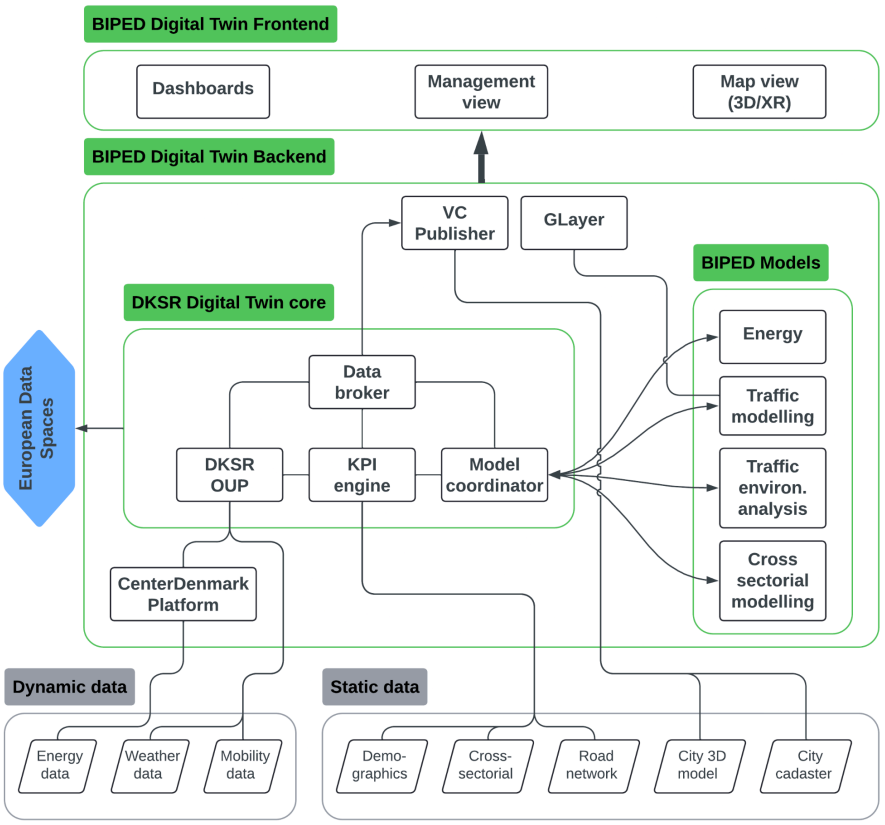

Figure 1. BIPED Digital Twin architecture - from deliverable D2.1

Deliverable D2.1 provides further descriptions of frontend and backend components. It is not necessary to replicate that detail here as the guidance provided is generally applicable to various types of backend and frontend applications.

There are two other areas relevant from ethical and legal compliance perspective:

- **stakeholder engagement**, which is essentially extraneous to the LDT environment but necessary to ensure the right kind of feedback from and impact on local communities in the area where the LDT is implemented. Deliverable 3.1 (BIPED Community) describes the stakeholder engagement in detail.
- **monitoring and evaluation**, deliverable D4.1 (Evaluation Action Plan and Reports) describes BIPED monitoring and evaluation aspects in detail. By building the privacy&ethical impact criteria into the data collection sheets in cooperation with the responsible partner (KPMG), this should ensure that the privacy&ethical aspects are on radar for purposes of monitoring and evaluation of the project progress and results.

3. Why privacy and ethical issues matter

What follows is a brief overview of ethical fundamentals that have horizontal application in areas where technologies play a key role and rely on (big) data.

In the world of disruptive technologies, legislation cannot always keep pace with the developments. It is therefore up to stakeholders to also proactively adapt and develop standards that are higher than minimum legal requirements.

Luciano Floridi and Mariarosaria Taddeo (2016)[2] defined three components of "data ethics":

- the ethics of data (how data is generated, recorded and shared);
- the ethics of algorithms (how artificial intelligence, machine learning and robots interpret data)
- the ethics of practices (devising responsible innovation and professional codes to guide this emerging science).

Ethics are both the foundational principles of legal norms and the basic guide for their interpretation, but also as ethical norms applicable to situations, which are not specifically regulated by legal rules.

There are at least three concurrent principles that shape that boundary and relationship:

- Ethical principles provide the foundations for the creation of legal requirements.
- No solution can be considered as "ethical" unless it also meets the applicable (minimum) legal requirements. In other words, there are limited grounds to argue that a solution which fails to meet the minimum legal requirements should nevertheless be allowed because it serves a particular ethical purpose.
- Legal requirements set the minimum standard, while ethics can be more aspirational and seek to impose a higher or the maximum standard. In other words, just because a solution is legal does not mean that it is the right thing to do.

Another level of differentiation may be observed based on the specificity of legal and ethical standards.

- General ethics - specific laws. Ethics may guide individual actors to do what is right in all aspects of life, while the law may provide rather more specific rules on how to execute such actions.
- General laws - specific ethics. The law may include a wide delegation to individual actors (natural persons, private entities, public authorities) to make a specific decision on an ethical basis. An example of this may be the legal delegation of ethical decision-making to individual practitioners and healthcare services providers by the medical legislation.

Areas of interest

There are several areas that typically pose challenges in projects around new and disruptive technologies:

- **Privacy** - discussing the risks of re-identification, risks of location data resulting in the processing of highly sensitive personal data, difficulties with obtaining data subject consent and other legal grounds for data processing in a smart city context; and the purpose limitation principle and risks of function creep. While the essentials of this

[2] What is Data Ethics? Phil. Trans. R. Soc. A, Volume 374, Issue 2083, December 2016, SSRN available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2907744

topic are covered by the DMP, this deliverable seeks to offer a more advanced good practice in selected areas such as location or soft data, or explain potential consequences of non compliance. Specific issues are raised by combinations of datasets, which can lead to re-identification problems and exacerbate the privacy risks. On the other hand, the deliverable makes clear that where no personal data is involved and there is no significant risk of re-identification, the GDPR framework does not apply and adhering to it may lead to overcompliance and sub-optimal allocation of resources.

- **Security and integrity of the digital twin and datasets.** This topic is essentially covered by the DMP and by the technical deliverables. This deliverable looks at several specific areas where it offers good practice, such as simple audits for partners to check that the factual and legal quality of the data is adequate, or to increase transparency in how the data is processed.
- **HPC (high performance processing), algorithms, data models and AI** - there is a scale on which the problem of opacity (black box) increases. There can never be a legally and ethically compliant solution unless the owner/provider fully understands the workings of its models / products (such as LDT) and its implications. The fundamentals of this issue are covered by the DMP. As the DMP explains, no high-risk AI models are intended for use in the BIPED LDT.

Inspiration from previous legal & ethical guides in digital twin context

Annex A reproduces guide principles that were developed as a deliverable in the Horizont 2020 Digital Urbat European Twins (DUET) project (grant agreement No.870697). This horizontal guide was based on frequent questions that digital twin builders and users face when implementing the twins and so may be directly helpful for BIPED. BIPED has many specificities however that are not captured by such horizontal guides and these are further deep dived in this deliverable. But it may be beneficial for partners across the board to familiarize with the guide.

4. Data layer

4.1. Personal vs. non personal data

Datasets and models that involve personal data warrant a different approach to compliance from datasets that involve no personal data whatsoever. Processing of personal data triggers the full-blown GDPR framework requirements, which cover all areas including legality and legitimacy of processing, data integrity and security, transparency and portability, and consequences and mitigation actions when a data breach occurs. The DMP reiterates the main rules and ties that to the BIPED data management lifecycle. At each interest area / best practice discussed below, this deliverable seeks to identify possibilities that personal data may be involved and recommend an action.

On the other hand, processing of non-personal data does not need to comply with GDPR and actually complying with all aspects of GDPR could lead to overcompliance and sub-optimal allocation of resources. However, different aspects come to the forefront, such as data integrity, security and IP rights management. These are further deep dived by this chapter is subchapters Staying compliant with license requirements, Data factual quality (properties) and Data legal quality.

Question whether the GDPR is applicable is clear in most cases, and the BIPED LDT is being designed in a way that the datasets used should not trigger GDPR application, aside from one set of working tasks, which is the stakeholder engagement. However, because LDT involves interaction and combination of datasets, this deliverable deep dives the issue of possible re-identification that can have both major privacy and ethical impact. Accordingly, this deliverable extend the DMP by providing some preliminary analysis of possible privacy & ethical impact of data combination, and description of the main re-identification risks (these are covered by the Front-end section).

4.2. Role of Data Protection Officers (DPOs)

As explained above, privacy being the cornerstone of ethical compliance in tech-driven projects and areas, the role of Data Protection Officers (**DPOs**) is key.

The primary role of the data protection officer (DPO) is to ensure that his/her organization processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.[3]

Under the GDPR, there are some types of organizations that must appoint a DPO[4]:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 of the GDPR (see also BIPED DMP) and personal data relating to criminal convictions and offenses referred to in Article 10 (this is mostly irrelevant for BIPED).

[3] https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en#:~:text=The%20primary%20role%20of%20the,the%20applicable%20data%20protection%20rules

[4] Article 37 GDPR.

The GDPR further lists certain sensitive activities that require a "data protection impact assessment" in which case the DPO must advise the controller when making such impact assessment[5]:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural no person;
- processing on a large scale of special categories of data referred to in Article 9(1) (see BIPED DMP), or of personal data relating to criminal convictions and offenses referred to in Article 10 (again, mostly irrelevant for BIPED); or
- a systematic monitoring of a publicly accessible area on a large scale.

Accordingly, a number of BIPED partners have a DPO by default and they should get involved in the project properly and in a timely manner in issues of processing of personal data.

However, as mentioned above and in the DMP, the BIPED project is not focused on primarily integrating personal datasets (aside from the stakeholder engagement line of tasks). It is therefore not strictly necessary (and in practice not the case) that a DPO is among the core project team members of BIPED partners. That said, it is recommended that:

1. DPO is aware of the main legal and ethical fundamentals and has been provided with a copy of the BIPED DMP.
2. BIPED project teams have a working relationship with the DPO and the legal team that enables prompt action and interaction when needed.

The dedicated legal & ethics partner (UTR) will seek to hold at least one joint meeting among the DPOs to facilitate implementation of these rules and best practice.

There are certain typical issues and pitfalls with using data (especially big data) to power a tool that may impact policy making.

4.3. LDT related issues

On top of the fundamental legal rules and recommended practice already described by the BIPED DMP, there are several further issues that deserve attention of this deliverable and implementing them will enhance the ethical compliance of the BIPED LDT and results. This section further picks to discuss and suggest best practice on the following topics:

- sourcing of data from third parties
- complying with license requirements in various scenarios
- ownership issues in cases of datasets
- data properties (factual quality)
- data legal quality

Cornerstone to all these topics is the privacy-by-design and by-default principle. The BIPED DMP provides that

The following subsections provide best practice to tackling each category.

[5] Article 35 GDPR.

4.4. Sourcing from third parties - minimizing the privacy risk

As described by the BIPED DMP, the majority of data to power the LDT will be sourced from third party providers. A simple check is recommended to map the potential privacy&ethics risks:

1. When you know you are sourcing **personal data,** ask specifically for the legal basis and the permitted purposes for which the data may be further used (re-used). Engaging your organization's DPO is recommended to confirm that the personal data may be sourced and further processed by your organization, including for purposes of the BIPED Project.

2. When you seek **non-personal data that have been through the process of anonymisation, aggregation or randomization**, ask specifically what measures / data sanitization techniques have been used for anonymisation, pseudonymisation or aggregation. This will help you assess the possible risks in their further combinations with other datasets.

   On the top of anonymisation issues described by the DMP, one particular pitfall exists in the question whether data can be considered anonymised and therefore not personal data: if the originator party (data controller) provides anonymised or aggregated data to a third party recipient (such as BIPED), but keeps the original (raw) personal data or the identification keys, the anonymised or aggregated data may still need to be treated as personal data. WP29 opinion 5/2014 on Anonymisation Techniques[6] stressed that:

   - "it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data. Only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous.
   - For example: if an organization collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data."

Ideally, the organization that has provided the data would guarantee that anonymized data is truly non-reversible.

4.5. Staying compliant with license requirements

Closed or proprietary (commercial) licenses: Copyright, neighboring rights, database rights and other IP rights over particular content (data, database, simulation model/software) mean

[6] ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 05/2014 on Anonymisation Techniques, April 201 4, p. 9., available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

that the right holder has the exclusive right to commercialize the content and decide with whom the content can be shared, how it is used, etc. If you seek access to such content, the only way is to negotiate and conclude a license agreement, or place a purchase order, with the right holder that will define the terms and conditions of your use of the database/model. Individual license agreement negotiations, where they are necessary, are typically done with the help of cities' legal departments or outside legal counsel, as they can involve quite complex issues.

As mentioned in the DMP, the majority of databases and models indicated for BIPED appear to be provided on an open-license basis, such as Creative Commons 4.0 ("**CC**").

The right holder (third-party provider) under such license grants you a worldwide, royalty-free, non-exclusive license to "use" the dataset or model for the duration of any applicable copyright or other IP rights (e.g., database rights), without the need to individually and ad-hoc negotiate these license conditions or place any purchase orders. In addition, an open license will contain few if any obligations or limitations imposed on what you can do with the licensed content.

An "Open" license will include the following "baseline" rights (see the "Open Definition" https://opendefinition.org/):

- extraction and re-use (or re-utilisation) of the whole or a part of the data in the set or model,
- creation of derivative datasets,
- creation of collective datasets (i.e., combining datasets),
- creation of temporary or permanent reproductions by any means and any form of the dataset,
- communicating to public (within the meaning of IP laws) of the dataset

Some Open Licenses may nevertheless place obligations on the data user:

- Attribution (e.g. **CC BY**) - you must give the licensor (or the original creator/author) the credit (attribution) in the manner specified by the license. For example, all Creative Commons licences require attribution except for the CC0-public domain variant.
- Share-alike (e.g., **CC SA**) - you may share or distribute derivative works only under a license identical with (or not more restrictive than) the original open license.

It is important to understand that the widely used "Creative Commons" licenses include both open and non-open types. The mission of Creative Commons is "Provide Creative Commons licenses and public domain tools that give every person and organization in the world a free, simple, and standardized way to grant copyright permissions for creative and academic works; ensure proper attribution; and allow others to copy, distribute, and make use of those works." However only the CC0, CC-BY and CC-BY-SA licenses are regarded as open.

Typical license restrictions to look out for in other Creative Commons licenses (and in licenses from other sources

- Restricted data use or sharing purposes, (e.g, CC-NC – only noncommercial uses of the work are permitted)
- Restriction on derivative works (ND) (e.g., CC-ND – no derivatives or adaptations of the work are permitted)
- Restrictions on combination with other datasets (see also section Back-end below).

License conflict: note that two or more separate licenses (for different datasets) may impact or even prohibit the possibility of their combination with other datasets, or their joint communication vis-a-vis third parties or the general public. This can be the case even with

Open licenses: for instance if dataset A is licensed under Creative-Commons-Attribution and dataset B is licensed under Creative-Commons-Attribution-ShareAlike then a combined dataset would have to have the ShareAlike condition applied to any re-use of that data.

Complex questions arising in the context of combination of datasets with different license conditions should be resolved with the help of your legal department.

Bear in mind that other interests than intellectual property rights may get affected by publication of data, whether the data is accurate or inaccurate. For example, economic interests of third parties may get affected if the publication of data showing high pollution levels happen to depress real estate prices. However, it may be difficult to consider such potentially remote risks at the stage of data selection by city officials. As a rule of thumb, if the data you publish is accurate and up to date, it is less likely that your organization would be held liable for any damages caused by the publication of such data (for example, damages that a real estate owner might claim if the price of its property deteriorates allegedly as a result of your organization publishing pollution levels data). Conversely, publication of inaccurate or incorrect data would increase the likelihood that some liability for damages may arise. Also other considerations than legal liability may impact your selection and use of databases or models, such as ethical consideration set out throughout this deliverable.

4.6. Ownership issues (decision, data, IP)

Decision ownership is key for distribution of responsibility and (legal) liability for the decision to be made. Multiple factors may indicate or affect ownership from the legal perspective: data ownership, IP ownership; AI ownership. Liability distribution is particularly difficult in complex decisions involving multiple actors or complex IT systems.

In practice, the decision owner and data/rights owner and user may be one and the same organization, but many other possibilities exist. For example: organization X may be the decision owner (e.g., determines the purposes and means of the data-based decision making, it would be the “controller” in the GDPR sense ; organization Y owns the data but makes them available for use to X; and organization Z may be “using” the data on X’s behalf (it would be the “processor” in the GDPR sense).

The BIPED DMP sets out specific rules for cases in which the BIPED partner is the data owner and in which it merely seeks to utilize data owned by a different partner organization. Unless this is clear at the outset with regard the datasets for BIPED, the partners ought to clarify ownership issues upfront.

4.7. Data factual quality (properties)

Data quality has a direct impact on the quality as well as legality of the decision or the decision-making process that are based on. Before implementing a dataset into an LDT, consider:

- Data properties:
    - relevance: the usefulness of the data for the specific decision-making process,
    - clarity: the availability of a clear and shared definition for the data,
    - consistency: the compatibility of the same type of data from different sources,
    - timeliness: the availability of data at the time required and how up to date that data is,
    - accuracy: how close to the truth the data is,
    - completeness: how much of the required data is available,
    - accessibility: where, how, and to whom the data is available or not available (e.g., security).

- Is personal data involved? When processing personal data, ensuring that the data processed is relevant, up to date, accurate and secure is mandatory by law (see GDPR principles of data minimisation, accuracy, and integrity and confidentiality).

- P*ractical example with ANPR (automated number plate recognition) data*: There are significant amounts of information an ANPR (automatic number plate recognition) system can collect. For example, is the system just recording vehicle registration marks? Or is it recording images of vehicles, occupants or 'patch plates' as well? If it's the latter, make sure the amount of information being collected is justifiable.

4.8. Data legal quality

Data, datasets and models may suffer from various legal defects. If defective data is used to power an LDT or drive decision making, the product or decision making chain may become tainted with risk of regulatory non-compliance, or the use of defective data may cause the decision-making process to become flawed and lead to wrong (harmful) decisions, thus creating a causal nexus between defective data and harm caused.

Typical legal defects:

- data collected or processed in breach of the GDPR or ePrivacy legislation (e.g., personal data collected without sufficient legal basis; non-anonymized location data shared by telecom operators, wrongly anonymised data);
- data acquired or processed in breach of licensing conditions (contractual breach), or without sufficient license (e.g., misused, stolen data);
- use of data infringing Intellectual Property (IP) rights of a 3rd party.

The steps you should take to check against these issues depends on your role vis-a-vis the data set:

- **Original data**. Your organization is primarily responsible for legal compliance of such data. This should be primarily achieved through compliance with the data collection requirements laid down by the BIPED DMP. Prior to using original data, check that they are defects-free to reduce any residual risks.

- **Existing data**. The following complements the general guidance of the BIPED DMP: In case of reuse of existing data, i.e. owned by someone else (a third party or another BIPED partner), the individual or joint responsibility is to check the nature of data and take the following steps:

    a. **BIPED existing data**. If unsure about legal compliance of this data, check with the data providing partner organization. If unsure about GDPR-compliance of your organization's existing personal datasets, conduct a data audit. This should involve identifying:
        i. categories of personal data you process;
        ii. location where it is stored (hard disks, cloud drives, physical filing cabinets);
        iii. inflows (sources of personal data – cameras, sensors, web forms, email, phone calls);
        iv. outflows (third parties with whom you share data – public authorities, private enterprises, individuals, cloud storage companies).

        → engage your DPO to oversee the audit

b. **Existing third party data** .
   i. 3rd party responsibility. Third party organizations should primarily be responsible for the data they shared. Therefore, you may make a careful assumption that the data, when provided for further re-use, is free from legal defects, because the 3rd party provider/vendor is obligated by law to collect, process, and share data lawfully and for legitimate purposes only. This assumption may not apply, however, if the data provider is established outside of the EU, because it may be subject to lower legal standards.
   ii. Limited data audit. It may be practically difficult for a decision-maker to review the entire history of an acquired dataset. However, a limited data audit may help decrease the residual risk:
      1. Does the data come from a reliable source? (reputable vendor or a public authority). Does the data come from a provider established in the EU?
      2. Doesn't the data suffer from defects in important properties? (accurateness, timeliness, consistency, etc., (see also Data factual quality (properties))
      3. Isn't the data manifestly unfit for the required purpose?
      4. Is the data shared under reasonable licensing conditions?
      5. Are there issues with correct anonymization or pseudonymization? (If you processed non- or insufficiently anonymised personal data by accident → engage your Data Protection Officer)
   iii. Licensing conditions. Further use of data may be limited by licensing conditions. This may include limitation of use purposes, manner of processing, data retention periods, or possibilities further to share or disseminate the data.

4.8.1. Location data

LDTs frequently rely on location data to track or count the number of people or vehicles in a given area. What follows is a deeper dive into typical issues with this data:

Location data. → Work with anonymous data, where possible (anonymised data preference principle). There may be different concerns depending on the data origin:

Telecom providers. Less risk with data acquired from electronic communication services providers. They are obligated by law to anonymise location data before sharing them with 3rd parties. Such anonymous data can be re-used for further processing, including for modeling purposes.

Location data collected from users' terminal equipment (see BIPED DMP for definitions). You may collect such data, e.g., by help of an app installed or cookie placed on an end user's mobile phone, → you are primarily responsible under the law for lawful collection and processing of such data. Any further processing (i.e. not the initial processing strictly necessary to provision of the end-user service/app) of non-anonymised location data is only possible with the terminal equipment's end user's consent (an additional consent with any such further re-use), or based on an exception provided for by the law → engage your DPO.

Possible flaws in anonymisation of location data. Seemingly anonymous location data may be vulnerable to re-identification. If your organization is handling the anonymization process → consult EDPB Guidelines 04/2020 on the use of location data and contact tracing

tools in the context of the COVID-19 outbreak.[7](The European Data Protection Board recommends conducting a reasonability test, which takes into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the GDPR).

Statistical counting/device fingerprinting. The above principle (user consent required) currently also applies to activities such as tracking of physical movement by scanning of users' equipment's Wi-Fi interface or other unique identifiers (such as MAC address, which is typically considered as personal data). Legal necessities in this area may change (relax) in the future, however, so if you engage in such data collection activities → discuss with your Data Protection Officer. Consult appropriate guidance (WP29 Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting[8]).

Floating car data (FCD). This time stamped geolocation and speed data may originate in connected vehicles (e.g., via their communication with the GPS or via mobile network connection). Collecting such data may trigger application of the ePrivacy rules (location data is collected via electronic communication service, or by accessing data on users' terminal equipment - mobile phone or the connected vehicle). Processing of anonymised FCD data should typically raise no issues, but beware of flaws in anonymisation.

Automatic Number Plate Recognition data (ANPR). ANPR data will be considered personal data to the extent it allows a vehicle and the related information (location, speed, photo of the driver) to be tracked to its registered owner, operator or the driver. Other data from the number plate recognition database may include vehicle type, fuel type, euro norm, CO2 exhaust, or weight category. Processing ANPR data fully anonymised should not raise privacy risks, but there may be specific cases in which they can (typically, if the anonymisation suffers from the "singling out" issue.

Sensitive data. HPC processing of location data may allow the data controller to draw far reaching inferences from the data, which reveal, e.g., life habits of data subjects. This creates risk of processing of special categories of personal data without sufficient legal basis. If you suspect this may be the outcome of your decision-making process → engage your Data Protection Officer. Note that where location data processing falls in scope of ePrivacy rules, there may be various country-specific differences in how that legislation has been transposed into the applicable laws.

4.8.2. Soft data and smart data

As described by the BIPED DMP, soft data may come from a variety of sources such as surveys but recently also from scraping of web data. The following provides additional best practice how to implement

Web / social media scraping ("voluntary data"; public registries of persons). This is typically personal data.

→ engage your DPO. Data Protection Impact Assessment may be required for large-scale data processing. Posting on social media publicly does not give third parties sufficient legal basis for further processing of the published data without informing the data subjects.

Best available legal bases may be:

---

[7] Available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

[8] Available at https://www.dataprotection.ro/servlet/ViewDocument?id=1089

- Processing is necessary for compliance with a legal obligation to which the controller is subject. This will typically be available for public authorities and other bodies entrusted with public administration tasks.
- 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. Potential argumentation lines include: public safety (e.g., municipal traffic management), economic well-being (e.g., optimization of services of general interest such as electricity, water and waste management), public budget interests. This set of examples is not exhaustive.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- Data subjects' consent. There are country-specific differences in minimum age for statutory legal capacity to give valid consent with personal data processing (Belgium: 13 years, Czech Republic: 15 years, Denmark: 13 years.[9] It is generally advisable to avoid scraping under age minors' data from the web, unless this is objectively justified, e.g., by the specific purpose of the decision/policy.
- You may be required to provide certain information to data subjects.

Personal data from public registries (open data). Open data legislation at the level of EU Member States may provide a list of documents or public data that may contain personal data (typically public registries), but which can be freely re-used for commercial or non-commercial purposes. No or low impact on data subjects' fundamental freedoms and interests is typically presumed in such cases. If unsure whether you can re-use personal data in public registries → check with your Data Protection Officer.

Smart data. Smart data are datasets extracted from larger amounts of data using algorithms (see also BIPED DMP definition). Self-check questions: do I understand the algorithms and underlying (raw) dataset used to produce the smart data? Are these algorithms fair? If you consider that the algorithms/machine learning processes or raw data used to generate smart data:

- are manifestly intransparent, unfair, suffer from obvious factual or legal defects, have wrongly set parameters or flawed methodology → escalate the issue to appropriate role within your organization, engage your Data Protection Officer or a legal officer
- contain personal data that may have been processed incorrectly/unlawfully, you have suspicion of a personal data breach → engage your Data Protection Officer

4.9. Who is responsible for defective data and their impact on models?

This short overview may help with understanding how legal liability may accrue in case there are flaws in dataset quality.

As a matter of principle, data owner/provider should be liable for the quality (factual, legal) of the data. Its use in your decision-making, may, however, bring your organization within the scope of liability rules, if, for example, a third party relies on your decision or on the way the decision presents the data, and suffers damage.

Examples of factors (co-)determining liability: whether data is integrated into software –

[9] https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf

- purely digital product (e.g., a licensable data model solution); whether data integrated into a device – product with some “physical existence” (e.g., a robot driven by data/software); whether data only used to inform a particular decision or a decision-making process.
- Contractual liability. Where your organization has a contract with the damaged party (e.g., licensee of your data model solution), it is likely that claims for damages linked to flawed data or flawed decision-making process will be targeted at your organization. Further rights of redress against the flawed-data provider may be available to your organization under the applicable law.
- Non-contractual liability. Where no contract exists between your organization and the damaged party, assignment of liability may be complex and there may be several extra-contractual liability regimes applicable in different EU Member States (as well as worldwide) at the same time. → engage legal officer at your organization if concerns exist

How to decrease risks of contractual or non-contractual liability:

- Impose appropriate licensing conditions, warnings and liability limitations on the recipients of your decisions (e.g., users of data model). For example, liability limitation clauses may be included in your contracts with third parties. Liability limitations may be imposed in open access licenses as well.
- Comply with license conditions and limitations attached to the data used. Make sure that these conditions and limitations are transposed further (e.g., attached to the software or data model) if applicable to the use of your products by third parties.
- Risk-shifting agreements (e.g., insurance contracts) may be available to cover impacts of your decisions/products. (Note that an obligatory insurance scheme for certain categories of AI/robots may be introduced in the future.)
- Precautionary approach principle may be recommended particularly in cases of large-size data processing, which may cause wide-spread damage. → engage legal officer at your organization if concerns exist.

4.10. Proposed audit

The audit has been already carried out in the form of critically analyzing the dataset requirements for the BIPED project and reflected in specific rules provided by the DMP (Deliverable D1.3 the Data Management Plan).

No deeper audit is proposed to check that the data sourcing and use conforms to the license requirements and security measures - this would go beyond what the consortium management can effectively supervise. Compliance with these requirements should be primarily ensured by the consortium partners in line with the DMP and with support of their own DPOs / legal departments.

However, partners will discuss whether a targeted audit should be conducted with respect to crowd-sourced soft data, if any.

5. Back-end

5.1. Further data processing

Any data-driven modeling and/ or other processes such as decision making based on data may result in negative outcomes due to: (i) flawed objectives, values or methodology chosen for the particular process; (ii) flaws (factual, legal) in the data used for making the decision; or (iii) flaws in the further processing of data for purposes of the process.

This guidance seeks to clarify primary mitigators from the privacy and ethics perspective:

- Data flaws: (see section Data layer above). The following steps assume that data selected to drive the decision are free from any factual or legal defects, including that personal data was originally collected in line with the GDPR.

- Flaws in further data processing (modeling or combining with other datasets)
    - Is personal data involved? Further processing must fully comply with the GDPR. Three particular overarching principles (among others) must not be breached:
        - Lawful processing. The decision-making process is likely to be considered a separate kind of processing, for which the controller needs to have a legal basis under the GDPR. → engage your Data Protection Officer
        - Purpose limitation. The purpose of further processing must not be incompatible with the purpose for which data was originally collected. There are certain purposes which may be deemed compatible, such as scientific research or statistical purposes.
        - Data minimisation. Data for driving a particular decision must be adequate, relevant and limited to what is necessary in relation to the purposes of that decision.
        - Country-specific GDPR derogations. Individual EU Member States may derogate from certain GDPR rules for specific purposes, e.g., national security, defence, public security, prevention of crime, other important objectives of general public interest (monetary, budgetary and taxation matters, public health and social security), etc.
        - A suggested gap analysis consists of these steps:
            - Identify which EU Member States jurisdictions are applicable to your processing activities.
            - Conduct a gap analysis to understand what needs to be done to update your policies or decision making processes. It may be necessary to engage privacy law attorneys qualified in the respective jurisdictions to make a more detailed case-by-case

- **(Geo)location data** → work with anonymous data, where possible (anonymised data preference principle)
    - Flaws in anonymisation. Anonymous location data are vulnerable to re-identification.
    - Revealing sensitive information. E.g., HPC processing of geolocation data from connected vehicles may reveal life habits of data subjects, and create other far reaching inferences. This creates risk of processing of special categories of personal data without sufficient legal basis. If you suspect this may be the outcome of your decision-making process → engage your Data Protection Officer

  - Aggregate data carry less privacy impact risk. If aggregate data can be considered fully anonymized or de-identified, they are no longer personal data and the GDPR does not apply.

- **Personal data containers** (privacy-by-design and privacy by-default principles). Where possible, have data collected and processed by devices locally. For example, use sensors that allow anonymization (e.g. blurring of images, aggregation, geo/masking) at source or shortly thereafter.
  - The Telraam service / cameras[10] are a good example of privacy by design : Telraam interprets camera data to count pedestrians, cyclists, cars and lorries. The privacy-by-design solution, allows the owner of the device to only see the camera pictures when installing the device (to outline the camera) and only counts are transmitted to the central server. The raw camera data is not exposed to anybody (except during installation). For further details on video devices data issues, see EDPB, Guidelines 3/2019 on processing of personal data through video devices.
  - Note that personal data container solutions may not be feasible if cloud infrastructure is used to collect and process raw data from sensors/cameras

- **Risks related to data collected from sensors**. It is recommended to stay aware of these issues and adopt mitigators:
  - Sensor fusion risk. Combining sensor data or data derived from different sources may lead to better and more precise information than would be possible when these sources are working in isolation. Increased possibility of risk that there is insufficient legal basis for such advanced processing of personal data, or that the purpose limitation or data minimisation principle will be exceeded. In addition, raw data can later be combined with other data incoming from other systems (e.g. CCTV or internet logs). In such circumstances, some sensor data are particularly vulnerable to re-identification attacks.
  - Risk of excessive data collection. IoT systems often lead to excessive data collection compared to what is necessary to achieve the purpose. Processing this data further may breach the data minimisation principle.

- **Age of the data**: Historic data may be less impactful also with regard to persons' privacy or commercial sensitivity. Context and (near-)real time data may, conversely, be more impactful. This may not be true in specific cases, but it may be useful to consider sensitiveness of the data processed in your risk analysis.

5.2. Purpose limitation

Any data-driven processing and modeling will have its intended purpose. Identifying it will be necessary to deal with legal necessities for any personal data processing, but also serve as a benchmark against which to weigh the relevance and necessity of the data (even non-personal data) intended to be used (principle of data minimisation). Adhering to the purpose limitation principle helps to avoid the phenomenon of "function creep", which means use of data for a different goal than it was originally collected for. Ignoring this may result in a GDPR infringement (if personal data is involved) and may increase overall legal liability risks.

[10] https://telraam.net/en/what-is-telraam

- *Is personal data involved?* Personal data cannot be processed unless for a specific purpose (purpose limitation principle). Such a purpose must be specified (set prior to the processing), explicit (clearly communicated to the stakeholders, mainly the data subjects, at the time of collection/processing) and legitimate (must not follow illegitimate aims, such as unlawful discrimination). When re-using personal data for further processing (e.g., modeling) and decision-making, consider this:
    - Purpose must still be specified. This can be conflated with the phase of setting the objectives of your particular decision-making process/data model, but the purpose must still be sufficiently specified.
    - Check sufficient legal basis. If the original legal basis for data processing was consent, check if your current purpose was covered in the specified plausible purposes when the consent was given (at the data collection point). If not, a new legal basis must be identified (either a non-consent-based, or you may need to obtain new consents from the data subjects) → engage your Data Protection Officer.
    - New purpose compatibility check. If the new purpose is not covered by the original data subject's consent, further non-consent based processing is possible only if it fulfils the GDPR purpose compatibility check. You may need oversight or approval of your Data Protection Officer. The following questions must be considered:
        - any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
        - the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
        - the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;
        - the possible consequences of the intended further processing for data subjects;
        - the existence of appropriate safeguards, which may include encryption or pseudonymization.
    - Compatibility presumptions: for cases of personal data, the GDPR deems three purposes for further processing purposes compatible, i.e., no need to run compatibility tests for these. Note that the anonymised data preference principle should still be observed unless it would prejudice the processing purposes.
        - archiving purposes in the public interest;
        - scientific or historical research;
        - statistical purposes.
    - Country-specific derogations/exemptions: Individual EU Member State's laws may also provide various legal exemptions from the GDPR standards on data processing for the purposes set out below. Where an exemption may apply to your processing, establish all the jurisdictions in which this processing takes place in order to be able to run an adequate gap assessment. Member States

may change the law from time to time – it is advisable to keep track of concerned jurisdictions.

- freedom of expression and information,
- public access to official documents;
- national identification numbers;
- employee data;
- professional secrecy obligations;
- churches and religious associations.
- information to data subjects: the GDPR requires certain information to be provided prior to each new processing to the data subjects

- **Terminal equipment data.** (e.g., location data collected via a mobile app or from vehicles). Re-use of data obtained from users' terminal equipment is not possible only based on the GDPR purpose compatibility test. End users' additional consent must be acquired before further processing of such data[11], e.g., for modeling purposes. → engage your Data Protection Officer. For example, telemetry data, which is collected during use of the vehicle for maintenance purposes may not be disclosed to motor insurance companies without the users consent for the purpose of creating driver profiles to offer driving behavior based insurance policies.

- **Other data involved**. Even with no personal data involved, identifying purpose of data processing may be important to ensure:
  - Compliance with any data licensing conditions and limitations;
  - Ensuring only relevant and adequate data are used for the decision-making (data integrity and minimisation principle).

5.3. Data minimisation, adequacy of data use

The data minimisation principle is the essence of the privacy-by-default approach.

Only data that is necessary to attain a set objective should be used for modeling. Processing of any excess data is unnecessary, thereby creating unnecessary risks, which may vary from hacking to unreliable inferences resulting in incorrect, wrongful, and potentially dangerous decisions. This in turn may expose your organization to unnecessary risks. Measures should be put in place that ensure data minimisation by default.

- Self-check: Am I using the maximum amount/extent/detail of data necessary for the intended purpose? Have I considered a less detailed/extensive dataset to achieve the same result? Is the data actually suitable to achieve the intended purpose?
- Data granularity: both extent and granularity of the data (e.g. data relating to individual persons as against aggregate data) matter in the data minimisation assessment.
- Is personal data involved? GDPR makes the by-default data minimisation principle mandatory.

[11] This requirement is based on national legislation implementing the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications))

- Is the data granularity and amount justified for the intended use of the BIPED project? Are there safeguards in place for avoiding unnecessary data collection?
- Data minimisation and adequacy should be considered at each separate processing operation.
- Large-scale processing of personal data may require a Data Protection Impact Assessment → engage your Data Protection Officer

It is necessary to adhere to the principle data minimisation also when further processing is for the "compatible" purposes, i.e., archiving purposes in the public interest, scientific or historical research and statistical purposes

Privacy-by-default means that the controller must implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. This applies also for purely inside organization handling of data, see Article 15.2 of the Grant Agreement (*Processing of personal data by the beneficiaries): [...]The beneficiaries may grant their personnel access only to data that is strictly necessary for implementing, managing and monitoring the Agreement*).

Sensor data. Sensors often lead to excessive data collection compared to what is necessary to achieve the purpose (this may breach the data minimisation principle).

Recommended risk mitigators:

- Pseudonymization is a technical and organizational measure that the GDPR recognises can be helpful in safeguarding the data minimisation principle.
- Encryption and an anonymized/ aggregated data consultation process ("hybrid processing"). It should be possible to encrypt personal information in a way that preserves the ability to run queries on the encrypted data. Analysts can ask questions that link together personal data, but they only ever see anonymized or aggregated results.

5.4. Automated decision-making and Artificial Intelligence (AI)

Even though the BIPED DMP has found that no BIPED tool/model is likely to fall in the scope of an AI system as per the AI Act definition[12], it is worth setting forth selected good practices from the AI space. This is because many issues typical for AI in the narrow sense (black box / opacity problem, accountability, human agent issue, bias) are relevant for many automated decision making settings as well.

In the words of the Commission High-level Expert Group on Artificial Intelligence, it is necessary to "de*velop, deploy and use AI systems in a way that adheres to the ethical principles of: respect for human autonomy, prevention of harm, fairness and explicability. Acknowledge and address the potential tensions between these principles*"[13] More unpacked, the High-level Expert Group explains that these principles encompass:

- The principle of respect for human autonomy: The allocation of functions between humans and AI systems should be human-centric design and leave meaningful opportunity for human choice. This means securing human oversight over work

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (**AI Act**), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

[13] Ethics Guidelines for Trustworthy AI available at https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf

processes in AI systems. AI should support humans in the working environment and aim for the creation of meaningful work.
- The principle of prevention of harm: AI systems should neither cause nor exacerbate harm or otherwise adversely affect human beings. This entails the protection of human dignity as well as mental and physical integrity. AI systems and the environments in which they operate must be safe and secure.
- The principle of fairness: the use of Automated decision systems should never lead to people being deceived or unjustifiably impaired in their freedom of choice.
- The principle of explicability: this means that processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions explainable to those directly and indirectly affected. Without such information, a decision cannot be duly contested. An explanation as to why a model has generated a particular output or decision (and what combination of input factors contributed to that) is not always possible. These cases are referred to as 'black box' algorithms and require special attention. In those circumstances, other explicability measures such as traceability, auditability and transparent communication on system capabilities may be required, provided that the system as a whole respects fundamental rights. The degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate.

Codes of ethics for automated systems

As a good practice and before the regulation becomes fully effective and applied in practice, it is recommended to follow reputable codes of ethics for the use of AI and automated decision systems. The initiative has an ambition to develop codes of ethics not only for public authorities but also for private companies (which may be far more advanced and experienced in the use of AI systems). Consider the following principles suggested by the private sector and as enshrined by the Ethics Guidelines for Trustworthy Artificial Intelligence (AI):

- AI products should reflect "Invented for life" ethos, which combines a quest for innovation with a sense of social responsibility.
- AI decisions that affect people should not be made without a human arbiter. Instead, AI should be a tool for people.
- We want to develop safe, robust, and explainable AI products.
- Trust is one of our company's fundamental values. We want to develop trustworthy AI products. (we will explain more in detail trustworthy artificial intelligence in the next section).

Several approaches may be implemented:

- "Human-in-command" (HIC): In this approach, the AI product is used purely as a tool. At all times, people decide when and how to use the results presented by the tool. An example is when a machine helps people with classification tasks.
- "Human-in-the-loop" (HITL): In this approach, people can directly influence or change decisions made by an AI product.
- "Human-on-the-loop" (HOTL): This approach concerns those cases in which the parameters relevant for decisions are defined by people during the design process, but the decisions themselves are delegated to the AI product. The application allows those affected by the decision to appeal for review. This ensures that people not only define the parameters for decision making beforehand, but also check retrospectively whether the decision was carried out in the intended sense.

As noted above, the French legislation offers an example of a similar approach, based on the “human guarantee” principle.

High-Level Expert Group on Artificial Intelligence observed that in creating trustworthy artificial intelligence systems, different groups of stakeholders have different roles to play:[14]

- Developers should implement and apply the requirements to design and development processes;
- Deployers should ensure that the systems they use and the products and services they offer meet the requirements
- End-users and the broader society should be informed about these requirements and able to request that they are upheld.[29]

The Group adds the following non-exhaustive list of requirements:

- Human agency and oversight Including fundamental rights, human agency and human oversight
- Technical robustness and safety Including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility
- Privacy and data governance Including respect for privacy, quality and integrity of data, and access to data
- Transparency Including traceability, explainability and communication
- Diversity, non-discrimination and fairness Including the avoidance of unfair bias, accessibility and universal design, and stakeholder participation
- Societal and environmental wellbeing Including sustainability and environmental friendliness, social impact, society and democracy
- Accountability Including auditability, minimisation and reporting of negative impact, trade-offs and redress

5.5. Documenting and communicating use / selection of data

Under the GDPR, each controller or processor of personal data has an obligation to maintain record of processing activities under its responsibility.[15] This will of course apply to any BIPED partner when processing personal data.

However, recording processing activities even when non-personal data is concerned may enhance the transparency of the back-end operations to the benefit of both other partners involved in the project and setting up the LDT and ultimately its users and other stakeholders.

What follows is a set of suggestions for improving the documentation and communication of use / selection of databases and models in the BIPED data management lifecycle, also taking account of the FAIR principles..

The starting principle is again that the data ownership goes hand in hand with the responsibility for data management (BIPED DMP)

The suggestions for a centralized logging /ld be logged in, for example:

- When (on what date) the data sourcing approval processes were met,
- Effective database / model sourcing date (date of concluding the licence agreement, date of first access, date of downloading, date of last access),
- All data sanitization measures applied to the dataset (anonymisation, pseudonymisation, aggregation, statistical evaluation, metadata generation, etc.),

[14] High-Level Expert Group on Artificial Intelligence, “ETHICS GUIDELINES FOR TRUSTWORTHY AI” (2018), page 14.
[15] Article 30 GDPR.

- All other defined “uses” of the database (what is a data use? See DMP for definitions), e.g., integrating the data into the BIPED system, updating the data, using the data to make a decision. If necessary to decrease the burden on users, define a level of “significance” for database use. Only a significant use would trigger then need to create a log,
- AI- or automated system-related decisions (including the use of data to “train” an AI), use of the “Digital Twin Data Broker” to process and aggregate data,
- Data storage-related decisions (e.g., decision to upload to a Cloud-based service),
- Access to / use of a database or model by third parties (e.g., external BIPED testers, BIPED final users in the course of BIPED data management lifecycle).

Define and make mandatory reporting of other events and errors, for example:

- Data breaches, security incidences, or similar adverse events,
- Accidental data re-identification,
- Reporting of data getting outdated, data getting beyond the permitted time for their storage,
- Reporting of significant change of circumstance that may make a dataset / model obsolete or inaccurate.

1. Define when a sharing of data / model with other BIPED partners should be recorded, transfer of responsibilities under the logging system and the BIPED data management plan.
2. Reporting of gaps and data needs. Define ways to log into the system a particular issue with the data or the lack thereof: missing dataset type, missing dataset set or subset, missing updates.
3. Trust-building and transparency. The logging system should allow seamless communication about dataset / model selection and use processes with
   - BIPED partner organizations,
   - BIPED users and testers,
   - the general public (dissemination),
   - Stakeholders and users should be allowed and motivated to conduct prior consultations with respective partners regarding the data needs and gaps for BIPED user cases.
4. FAIR data principles: ensure full machine-actionability of the logs (findable, accessible, interoperable, reusable)

5.6. Proposed audit

Targeted audit is proposed once all the required datasets are procured and are being implemented by the technological part of the consortium into the LDT. The main focus of the audit would be various dataset combinations and whether they are duly processed within the LDT backend framework, with focus on certain highly sensitive areas (e.g. datasets with potential bias, soft data from web / social media scraping).

6. Front-end

6.1. User stories

At this stage, specific user epics / cases for the BIPED LDT are still under development. To the extent the front-end will be designed with specific user epics in mind, the privacy and ethical dimension will always be case-specific.

It is a recommended good practice to define user epics as precisely as possible, given the specific stages of a project and LDT implementation.

The following overview provides likely ethical consideration with respect to user categories as preliminarily defined by chapter 2.1 of BIPED Deliverable 2.1 Initial release of the Digital Twin Platform & Architecture

User Fact Sheet 1: Decision Maker

Purpose: Needs to make decisions at a strategic level in order to drive urban development forward efficiently, meeting the City's objectives.

User Stories:

- UR-1.1DM: As a Decision Maker, I want to know what influence a considered measure will have on the traffic itself, on traffic energy consumption and on the traffic environmental impact so that I can consider alternative measures and select the optimal one.
- UR-1.2DM: As a Decision Maker, I want to evaluate the performance of current heating infrastructure so that I can recommend upgrades and maintenance to improve efficiency and reduce emissions.
- UR-1.3DM: As a Decision Maker, I want to analyse heat demand forecasts so that I can identify areas for expanding the district heating network and to ensure that the future capacity meets the projected growth.
- UR-1.4DM: As a Decision Maker, I want to integrate weather data to forecast demand spikes during extreme weather conditions so that I can implement strategies to balance supply and demand, preventing outages and maintaining grid stability.
- UR-1.5DM: As a Decision Maker, I want to use temperature data to provide drivers with accurate EV range predictions so that I can optimize battery usage and ensure reliable vehicle performance in cold weather.

Likely ethical considerations:

- *Finding the best data / models for my decision making*
- *Understanding the possibility of selection bias in the choice of data and what is "best"*
- *Do I understand the data models? Am I able to interpret their results? Am I able to use the system?*
- *Do I trust the models?*
- *Am I not creating or perpetuating any bias toward any vulnerable groups?*

User Fact Sheet 2: Politician

Purpose: Needs to explain and justify decisions and measures taken in order to get a voters' confirmation of his/her politics.

User Stories:

- UR-2.1PO: As a Politician, I want to know how much closer we are to district energy positivity now than we were before I took charge of the district so that I can present how my political decisions helped the district.
- UR-2.2PO: As a Politician, I want to review the social, economic, and environmental benefits of the proposed twin so that I can advocate for policies and investments that align with my constituents' needs and the city's long-term sustainability goals.

Likely ethical considerations:

- *Reliability and integrity of the data that are underlying policy decisions*
- *Transparency towards citizens that their data is used, decisions made based on data concerning them.*

User Fact Sheet 3: Data Analyst

Purpose: Needs a data driven understanding of a real world phenomenon in order to help decision makers to make data driven decisions.

User Stories:

- UR-3.1DA: As a Data Analyst, I want to iteratively explore the history of traffic in the district so that I can look for spatiotemporal traffic patterns.
- UR-3.2DA: As a Data Analyst, I want to integrate various data sources related to urban heating so that I can provide comprehensive insights to decision-makers for strategic planning.

Likely ethical considerations:

- *Accountability and transparency - knowing and making known the origin of the data, respecting and passing on data limitations*
- *Data integrity and security*
- *Transparent and fair use of data models*
- *Privacy-by-design and confidentiality, risks of re-identification of anonymous data*
- *Setting front-end technical options (color modes, visualizations, diagrams, etc.*

User Fact Sheet 4: Citizen

Purpose: Needs to be informed about conditions which can affect his/her behavior in order to make conscious decisions driven by facts (data) instead of subjective feelings.

User Stories:

- UR-4.1CI: As a Citizen, I want to see the traffic in the district in real-time so that I can choose the appropriate mode of transport
- UR-4.2CI: As a Citizen, I want to understand how district heating will affect my utility costs and comfort levels so that I can support initiatives that improve my quality of life and align with sustainable urban development.

Likely ethical considerations:

- *How is my / my co-citizens' data processed?*
- *For what purposes?*
- *Is the data safe?*
- *Are any automated processes involved in the decision-making about me / using my data?*
- *Do I trust my city? Is the city transparent about its decisions and policies, and data management?*

User Fact Sheet 5: Community Engagement Officer of the City

Purpose: Needs visual instruments to foster citizen engagement as part of participatory processes in the context of Urban Planning.

User Stories:

- UR-5.1CE: As a Community Engagement Officer, I need a visualisation tool that I can use in participatory processes with citizens to clarify planning measures, e.g. compare designs.
- UR-5.2CE: As Community Engagement Officer, I need an easy to handle tool that I can interact with on-site and that allows me to quickly draw citizens' ideas onsite into the 3D-Map.

Likely ethical considerations

- *Do I understand the tools and models? Am I able to interpret their results? Am I able to use the system?*
- *Do I trust the tools?*
- *Am I not creating or perpetuating any bias toward any vulnerable groups?*
- *Have I chosen the right visualisation tools / color modes, diagrams etc?*

User Fact Sheet 6: Architects from private companies

Purpose: Needs a greater availability of data (e.g. shadow impact, energy consumption, mobility needs) to provide better designs.

User Stories:

- UR-6.1Arch: As an architect in the competition process, I want to have direct access to selected data sets in order to customise my designs.
- UR-6.2Arch: As an architect, I want to be able to test my designs directly in the virtual 3D model and better understand its impact.

Likely ethical considerations:

- *Do I have sufficient legal basis to access and use selected datasets?*
- *Do I trust the data source? Who is responsible for the datamodels?*
- *Data integrity - is the data up to date and accurate?*

6.2. Presenting results from combined datasets - privacy and ethics impact assessment

A common risk related to combination of various data datasets in large data models and tools is that the data has unforeseen ethical impacts or results in re-identification of what was considered an anonymised/statistical dataset and thus to a privacy breach.

This section intends to provide some theoretical background and on that basis provide a preliminary assessment of those risks on the basis of the identified dataset requirements for the BIPED project.

GDPR does not apply to non-personal data, i.e. data that does not relate to an identifiable natural person (data subject). However, processing of large amounts of data or aggregation of different datasets may significantly increase the risk of data re-identification. As set out in the BIPED DMP Article 29 Working Party's 2014 Opinion on Anonymisation Techniques[16] identifies the three common risks of re-identification:

- '**Singling out**': the "possibility to isolate some or all records which identify an individual in the dataset."

[16] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- **'Linkability'**: the "ability to link at least two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases)".
- **'Inference'**: the "possibility to deduce, with significant probability, the value of an attribute from the values of other attributes."

Risks under 2 and 3 appear particularly relevant if an LDT processes large datasets. Where the processing of data results in its re-identification, the GDPR becomes fully applicable to that data(set). The danger is typically in the fact that re-identification happens 'under the radar', resulting in a potential data breach and the unaware data controller being exposed to the risk of penalties for breach of GDPR provisions.

That said, the size of the dataset is not always a clear indicator of re-identification risk. A small dataset could be easier to de-identify because the data subjects are inherently from a small sub-group. The greater risk is a large number of attributes for each data subject, increasing the possibility that a separate set of attributes (e.g. age, geography, occupation, number of children) will identify a separate individual person. In addition, the risk of re-identification may not be spread evenly for the entire dataset - some cases may be identified while others remain anonymous.

The fact that the GDPR may become applicable to a dataset in which the risk of re-identification has materialized does not automatically mean that the organization handling the data may be penalized for unlawful personal data processing. In such cases, however, it is advisable that the organization handling the data takes all reasonable steps, seeks appropriate expert advice and applies all relevant professional standards in order to mitigate the risk of a privacy breach and further unlawful personal data processing.

In addition to pure privacy impact, combinations of datasets may have various, oftentimes unexpected ethical impacts. It is difficult to estimate all such potential impacts from one's desk. While this deliverable provides some examples, the best way to anticipate ethical impact is through discussion based on specific datasets and user epic proposals.

A set of examples of potential privacy and ethical impact of specific datasets selected for BIPED LDT is provided at Annex B - preliminary privacy and ethics assessment of possible dataset combinations, but here are the most prominent examples:

Dataset	Privacy/ethics impact?	Possible mitigator
Demographics: Population ethnicity distribution on household level	**Privacy**: Possible linkability problem in combination with other data (e.g. detailed geospatial point and public land registry data) may be able to reveal ethnicity of (re-)identifiable individuals or specific households. **Ethics**: Possible impact if LDT results portrayed with unfavorable connotations or LDT output can be used or misinterpreted to discriminate based on ethnicity.	**Privacy**: Aggregate front end display on a higher than single point level, e.g. street, cluster, section of the neighborhood. **Ethics**: Clearly define LDT user epics and roles and BIPED purpose / objectives for the front end display to minimize risk of misinterpretation.
Noise measurements on sensor level	**Privacy**: issues unlikely. **Ethics**: Linkability problem if combined with highly specific geospatial points, may allow precise identification of noise pollutants / source of noise.	**Ethics**: Make harder to identify specific noise pollutants in the widely accessible LDT model.
Location of district heating circuit lines and distribution system	**Privacy:** issues unlikely. **Ethics:** Hypothetical concerns from a	**Ethics:** These remote impacts may be difficult to estimate. In case of serious doubts, consult appropriate public

	strategic/defense perspective if the LDT significantly enhances precision of the provided information.	authorities

Table 1. Examples of preliminary privacy/ethics assessment

Demographics data on ethnicity distribution is a prominent example where combination with other datasets is likely to lead to a linkability problem that has both privacy and ethical ramifications. Data on racial / ethnic origin of identifiable individuals is a special category of personal data that is strongly protected under GDPR. As such, the BIPED LDT impact in this instance should be closely monitored throughout the project lifecycle.

Note that at this stage, this assessment has the following shortcomings and should be revisited at the following milestones

- BIPED LDT user epics are more clearly defined
- Data sets for BIPED LDT are procured and evaluated with regard to data quality and compliance as described in section Data layer above.

6.3. How to present LDT outputs

It is a notorious fact that the choice of color for presenting correlations or data analysis results is impacting the subsequent decision making.[17] It has therefore direct implications for ethics.

There are various opinions on what colors have what implications, which is in any event culturally and regionally specific.

Without an ambition to provide exhaustive guidance here, the LDT designers should bear this aspect in mind and when choosing the colors for tools available in the LDT front end, exercise caution. For example, they should avoid using colors generally having “aggressive” or “bad” connotations such as red, when dealing with data and results dealing with population’s ethnicity or social status. It may be recommended to use neutral colors such as shades of blue.

6.4. How to read the LDT outputs - making data-driven decisions

Datamodels and LDTs may inform decision-makers at various stages of a smart city development.

[17] For example Location and color biases have different influences on selective attention Jillian H. Fecteau a,b,*, Ilia Korjoukov a , Pieter R. Roelfsema, available in full here; see further Aparna Sundar, James J. Kellaris. How Logo Colors Influence Shoppers’ Judgments of Retailer Ethicality: The Mediating Role of Perceived Eco-Friendliness. Journal of Business Ethics, 2015 https://ideas.repec.org/a/kap/jbuset/v146y2017i3d10.1007_s10551-015-2918-4.html , or Colours’ Impact on Morality: Evidence from Event-related Potentials, Tian Gan, Wei Fang & Liezhong Ge https://www.nature.com/articles/srep38373

What type of decisions?

Consider the type, scope and status of the to-be-made decision. Properly name roles and assign responsibilities. This may all co-determine the legal requirements on a compliant decision-making and also impact on potential legal consequences of any problem with the decision or how data is used to drive it.

- Executive/operational/minor decision. Smaller scale decisions may be subject to less stringent or copious legal requirements and carry lower risk of legal liability. However, consider this:
    - Is personal data involved? GDPR is applicable at each step that may be considered processing of personal data. Even a single, isolated breach of GDPR may lead to enforcement and penalties, which can be very high and commensurate with the economic size of your organization. → engage your Data Protection Officer
    - At what level of the organization hierarchy is the decision made? An executive decision made high up may have wider impact and legal consequences down the line.
    - How is data presented? The way data is presented as the result of a decision-making process may influence future decision making processes, thus causing any potential issue to proliferate. → establish an escalation path to your superiors for cases where serious issues or threats of data breaches occur

- Policy/strategic/major decision. A wider impact decision can take the following forms: (i) organization-wide policy document, (ii) decision embedded or integrated in a data model, (iii) decision used for machine learning or to set parameters of an AI system, or (iv) document shared with or sold to third parties, or published to (or even made binding on) the general public. Such decisions carry higher risk, will typically have higher legal requirements, and may cause a more wide-spread damage. Consider this:
    - Is personal data involved? Large-scale operations with personal data may have a greater impact on data subjects' privacy. GDPR may require so-called "Data Protection Impact Assessment" to be carried out in certain high-risk areas:
    - Use of new technologies (e.g., Internet of Things applications[18]);
    - Systematic monitoring of a publicly accessible area on a large scale (including with CCTV cameras or sensors able to collect personal data);
    - Systematic and extensive evaluation of personal aspects based on automated processing, including profiling), and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
    - Processing on a large scale of special categories of data and data relating to criminal convictions and offences.

      → engage your Data Protection Officer. Consult appropriate guidance (Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679).
- Large-scale data = large-scale liability. Any issues with data properties quality or legal quality (e.g., data collected or processed in breach of GDPR or licensing

[18] Note that this may trigger applicability of other legislation than that mentioned by the BIPED DMP< such as the EU ePrivacy Directive (and the upcoming new ePrivacy regulation) or the EU Data Act. If relevant, do inquire the dedicated legal&ethics partner (UTR) for more details.

conditions) may proliferate in large-scale data operations, or when implemented in a decision with wider reach. Potential for organization-wide legal liability for regulatory non-compliance and any damage caused. → Identify the appropriate person/role/body within your organization hierarchy to make or approve strategic-level and policy decisions.

- Legally binding measures/policy imposing a limitation to the fundamental right to privacy. If you are a public authority and consider (and have the requisite power of) adopting a policy with legal (or quasi-legal) effects on the general public that also involves data processing, such type of decision may be subject to additional requirements imposed by EU and international law on states to ensure individuals' fundamental right to privacy. You may wish to consult the following step-by-step guidance: EDPS, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", 11 April 2017, and EDPS, "Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data", 25 February 2019.

Type of decision-making process

Human factor / manual decision making processes may be prone to human factor mistakes and lack of control.

- Is personal data involved? Purely manual, non-automated processing of personal data falls out of scope of GDPR, unless it is intended to form part of a "filing system" , or you create written records in a manual filing system.
- Difficult cases in distinguishing manual versus automated decisions: a model presents visualized data (e.g., based on running a query on the LDT system), and I make the decision on its basis. Is it manual or (partly) automatized? → the precautionary principle guides to adhere to the stricter legal and ethical standard, which in this case may mean that the decision making should comply with GDPR and higher standards for ensuring accountability, transparency and security of systems (see below).

Automated decision-making processes may be more demanding in ensuring accountability and transparency

- Is personal data involved? Automated processing of this data always triggers GDPR application. N.B. processing information in an electronic form (e.g., inputting data points into a computer software, such as MS Office) is considered automated.
- Risk of re-identification. When non-personal data goes through machine learning or deep learning processing, there is still a chance it can be linked to an individual person thanks to the advanced computational capabilities. Data can thus dynamically become personal data again.
- GDPR places special requirements on automated individual decision-making and profiling, which may produce legal or similarly significant effects concerning data subjects for example e-recruiting practices without any human intervention. Data subjects must be informed about such automated decision-making upfront. → engage your Data Protection Officer
- Only partly automated processes do not typically lower the standards required for the process, including legal necessities (e.g., GDPR remains fully applicable to the entire processing).
- Fully algorithmic/autonomous decisions: model makes the decision, I only implement. Currently, there are significant gaps in AI regulation.

6.5. Proposed audit

Once user epics are finalized and the LDT in advanced stage of development, a targeted audit should be conducted to check whether

- the user epics correspond with overall ethical aims of the project,
- the LDT is contributing to meeting those aims,
- evaluate the transparency of the front-end operations, especially with regards to how data sources and models are presented to users.

6.6 Audit as regards sourcing and use of district heating data (lessons learnt) (added in version 1.1)

In Period 1 of the Project, responsible partners led by DTU have conducted negotiations with Kredsløb, a district heating provider in Braband, to obtain data on heating / energy consumption.

Initially this Implementation Manual has foreseen privacy and ethical risk in possible linkability of such data: *Linkability may allow identifying individual consumption patterns if combined with highly specific geospatial points (and publicly available land registry data).* (see also Annex B - preliminary privacy and ethics assessment of possible dataset combinations)

This concern was shared by Kredsløb. The negotiations have resulted in providing a dataset that aggregated heating consumption datapoints at a lower spatial granularity. This has effectively mitigated any possible concerns that users could link consumption data with any specific household/building, while ensuring that the data still fulfils its purpose within the LDT to be able to map possible (in)efficiencies in heat parameters of specific areas.

7. Stakeholder engagement

Conducting stakeholder will almost always result in collecting personal data, only if names of stakeholder individuals and their contact details (email addresses, telephone numbers). The BIPED DMP provides specific rules on how to handle these.

But more importantly, the goal of stakeholder engagement is to obtain valuable insights of various individuals or of interest groups. Depending on the objectives and methods of the stakeholder engagement, and the samples surveyed, this may involve collecting of individual's opinion on political or other societal matters. Processing such data may have significant privacy and ethical impact.

Privacy aspects are covered by the DMP. As regards ethics, there is plenty of sources[19] on best practices how to ethically conduct surveys and interviews, which can be distilled into the following set of core principles:

- **Obtaining informed consent** from participants (see DMP and template consent forms)
- **Clearly explaining the purpose** of the survey (see DMP and template Study information sheet)
- **Ensuring confidentiality and anonymity** of the responses (see rules set out by the DMP)
- **Avoiding bias and leading questions**. Questions should be neutral, avoiding any language that might influence participants' responses. Leading questions, which prompt a specific answer, are strictly avoided to maintain integrity.
- **Respecting diversity**. Surveys should be designed to include people from various backgrounds, cultures, and demographics, providing a well-rounded perspective.
- **Data security.** Ethical surveys prioritize the security of the collected data. Robust measures are in place to prevent unauthorized access, ensuring that participants' information is protected from potential breaches (see DMP for details).
- **Transparent communication** Ethical surveys are transparent about the purpose, the organization conducting it, and how the gathered data will be utilized. Clear communication builds trust and encourages participants to engage openly (see DMP and template Study information sheet)..

BIPED deliverable 3.1 (BIPED Community) sets out the core principles for conducting stakeholder engagement. As it was developed at the time of the BIPED DMP, it is in-line with the main guidance provided therein. Stakeholder engagement activities should further align

[19] The professional bodies listed below, among many others, provide guidance on the ethical conduct of research and surveys.

- American Psychological Association: http://www.apa.org
- British Psychological Society: http://www.bps.org.uk
- British Medical Association: http://www.bma.org.uk.
- UK General Medical Council: http://www.gmc-uk.org
- American Medical Association: http://www.ama-assn.org
- UK Royal College of Nursing: http://www.rcn.org.uk
- UK Department of Health: http://www.doh.gov

See further summary here https://surveysparrow.com/blog/ethical-surveys/ or here https://academic.oup.com/intqhc/article/15/3/261/1856193

with the ethical framework set out in this deliverable and the responsible BIPED partners are encouraged to coordinate with UTR for this purpose.

Proposed audit: when the consortium conducts engagement with local stakeholders (citizens, communities & local interest group) as opposed to institutional or corporate stakeholders, audit to check how these stakeholders are handled in the engagement process and how the results are presented and incorporated in the LDT and BIPED results overall.

8. Conclusion and future work

This deliverable sought to identify a set of good practice for each of the stages of development of the BIPED LDT to ensure and maximize privacy and ethical compliance and contribute to mapping of these factors over the project lifetime.

While no future deliverable is envisaged under the proposal to, the dedicated privacy&ethics partner (UTR) will stay close at the project milestones to conduct targeted ethical audits in roughly the following structure:

- Data layer - the audit has been already carried out in the form of critically analyzing the dataset requirements for the BIPED project and reflected in specific rules provided by the DMP (Deliverable D1.3 the Data Management Plan). No deeper audit is proposed to check that the data sourcing and use conforms to the license requirements and security measures - this would go beyond what the consortium management can effectively supervise. Compliance with these requirements should be primarily ensured by the consortium partners in line with the DMP and with support of their own DPOs / legal departments. However, partners will discuss whether a targeted audit should be conducted with respect to crowd-sourced soft data, if any.
- Back end - to be carried out once all the required datasets are procured and are being implemented by the technological part of the consortium into the LDT. The main focus of the audit will be different dataset combinations and whether they are duly processed within the LDT backend framework, with focus on certain highly sensitive areas (e.g. soft data from web / social media scraping).
- Front end - to be carried out once user epics are finalized and the LDT in an advanced stage of development. The main goal will be to check whether
    a. the user epics correspond with overall ethical aims of the project,
    b. the LDT is contributing to meeting those aims,
    c. evaluate the transparency of the front-end operations, especially with regards to how data sources and models are presented to users.
    d. Describe enhanced stakeholder involvement not only as regards accessibility of BIPED front end to stakeholders, but how they are involved to inform development of specific user requirements and design of the LDT (added in version 1.1)
- Stakeholder engagement: when the consortium conducts engagement with local stakeholders (citizens, communities & local interest group) as opposed to institutional or corporate stakeholders, audit to check how these stakeholders are handled in the engagement process and how the results are presented and incorporated in the LDT and BIPED results overall. (Citizens, communities & local interest group) as opposed to institutional or corporate stakeholders, audit to check how these stakeholders are handled in the engagement process and how the results are presented and incorporated in the LDT and BIPED results overall.

Specific project timeline milestones will be identified for the proposed audits. Under the Proposal, no specific deliverable is expected to result from the targeted ethical audits envisaged by this deliverable, but partners responsible for individual project tasks will be expected to respect audit findings and implement necessary measures.

The legal&ethics partner (UTR) is organizing a meeting of partners' DPOs to discuss the fundamentals of the BIPED DMP, this deliverable and the planned audits.

9. Integration of EC Recommendations on D1.4 (added in version 1.1)

At the end of the Reporting Period 1 (RP1), the European Commission has provided the following feedback on D1.4 (EC Request for revisions Ref. Ares(2025)10702198 - 04/12/2025):

The deliverable is in line with the DoA. Overall, it is of good quality and it is acceptable. This is a living manual that specifies privacy-by-design for the local digital twin across data, backend, front-end and stakeholder layers, consolidating GDPR/EDPB guidance and linking to the DMP.

9.1 BIPED Consortium Response and Integration

The table below provides a summary of how the BIPED consortium has addressed the EC's recommendations. It indicates the actions taken, highlights the sections that have been marked in yellow within the revised document, and references where in D1.4 the added content has been integrated:

EC Recommendation	Consortium Response / Action Taken	Marked in Yellow	Location in D1.4
This is a living manual that specifies privacy-by-design for the local digital twin across data, backend, front-end and stakeholder layers, consolidating GDPR/EDPB guidance and linking to the DMP	A further iteration of the D1.4 will include description of BIPED's partners' activity as regards enhanced stakeholder involvement not only as regards accessibility of BIPED front end to stakeholders, but how they are involved to inform development of specific user requirements and design of the LDT. This iteration provides a new subsection 6.6 describing a lesson learnt in how to mitigate privacy and ethical concerns in sourcing potentially sensitive heat consumption data from a local heating supplier. This demonstrates the use of best practices for risk mitigation in similar scenarios.	yes	Executive summary Section 6.6 Section 8

Annex A - H2020 DUET project Ethical Principles for using Data-Driven Decisions in the Cloud (Grant Agreement No.870697) part of Deliverable D1.5[20]

Questions asked to digital twin designers and users

"I had been assigned a task and I was not sure whether I am allowed to use the data collected by my City for this purpose."

I was not sure whether my City has data available that would help me to complete a particular task. I was unsure who to turn to to find out."

"I felt that I lacked the skills and knowledge in data analytics / visualisation in order to use the available data to make a data-based decision."

"I had to rely on a result given by a data processing model to carry out a task or make a decision, but I was not sure whether the result was reliable."

"I wanted to use a data processing model but I was not sure that I understood fully how it works."

"When working with some data (e.g. noise, pollution), I realised that the data reveal the source or the cause of these externalities (e.g., the exact location of a polluter). I was wondering if someone may be responsible for committing an administrative offence (or even a crime) and I was not sure whom to contact about this. I was not sure whether I could make this data public, and what the reaction from the general public might be.

"I worked with anonymous data but after combining different data sources, they began to reveal information about identifiable persons (personal data)."

"I was working with a third-party provided dataset, but realized that these are actually personal, highly sensitive data (e.g., data showing individual people's health condition, or data allowing me to learn about a person what his/her religion or sexual orientation is). I wasn't sure about whom to contact and what to do with the database."

"We cooperated with a private organisation (a firm, company, non-profit) on a joint task. The private organisation planned to collect some data in the course of the task. I was not sure whether the organisation could share the data with us. I was not sure how to ask that

[20] https://www.digitalurbantwins.com/_files/ugd/725ca8_7aa91c5355244134878940fe16e093b9.pdf

organisation to share the data with us. The organisation refused to share the data with us and I didn't know what to do."

"I wanted to present some data with help of visualisation but the system won't allow me to choose the colour I want or a type of visualisation that would work best in my opinion."

The ensuing guide / principles:

1. **Accountability and data sovereignty**

   1.1. Know the origin of the data, its lawful and ethical uses, and any limitations on their sharing or publication.

2. **Transparency**

   2.1. You should know what data you collect and for what purposes.

   2.2. The data subjects (e.g. the citizens) should know what data you collect about them and for what purposes.

   2.3. Be transparent about the scope and source of the data, as well as the limitations of the data. Explain what information the data contains, how (and where) it was collected, whether it is static data, updated regularly, or real-time.

   2.4. If the data is publicly available, provide a link to the data repository/source url.

   2.5. Make sure that decision makers are aware of the deficiencies / limitations of the data.

3. **Data quality**

   3.1. Get the best data as you can for your purposes. Best may mean:

      3.1.1. data most suited for your purpose;

      3.1.2. most complete, correct, and up-to-date data (clean data);

      3.1.3. data with a transparent track record of their collection, storage, and the log of previous processing;

      3.1.4. data with a clear licence to (further) use.

   3.2. Take active steps to ensure and maximise the quality, objectivity, usefulness, integrity and security of data.

4. **Data quality for publication**

   4.1. If the data is sufficient for an internal use (within the services of the city), it is

typically equally good for making the data publicly accessible (open).

4.2. Use open standards and open licenses.

4.3. Publish data only after you have cleared the applicable legal requirements.

5. Data security

5.1. The integrity and security of data should be maximised.

5.2. Use trusted third-party services providers (e.g., approved by the future European Union.

5.3. Cybersecurity Certification Scheme on Cloud Services (EUCS)).

6. Data everywhere

6.1. Promote the use of data in public interest, be active in seeking out data that may be (re)used in public interest.

6.2. Actively explore the ways in which data can be obtained from partners (private or public) with whom you engaged in a joint activity (e.g., public procurement).

7. Transparent and fair use of AI and computer models. Fighting the "opacity" problem.

7.1. Cities should strive to develop the officials' ability to understand, interpret and use automated decision-making systems. They should understand at least the basics of the underlying algorithms and the data used. This can be achieved by a targeted education and training, for example.

7.2. Data subjects (citizens) should be informed about the fact that automated decisions are being taken about them and with the help of their data. To the extent possible, cities should strive to make sure that data subjects also understand the underlying algorithms, to the extent practicable.

7.3. Algorithms and automated decisions should be fair and proportional. They should not prejudice the data subjects. Even though some bias may be inherent in data, the algorithms and the data they use (or train on) should not create or perpetuate material biases (racial, ethnical, sexual, political, religious, etc.)

7.4. Ensure an element of human control over the AI:

7.5. Individuals to whom human oversight is assigned should fully understand the capacities and limitations of the AI system and should be able to duly monitor

its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible.

7.6. Data subjects should be granted the right to appeal relating to data processing and
the automated decisions that affect them.

8. Presentation of data or results

8.1. The way data or data-based decisions are presented should avoid creating or perpetuating bias (e.g., the use of red and green color coding for visualisations).

9. Data ownership and management

9.1. Data ownership typically goes hand in hand with the responsibility for data management.

9.2. Third parties contracted out for city data management should be chosen responsibly, adequate data processing agreements should be put in place.

10. Privacy-by-design

10.1. Comply with all legal requirements when acquiring, using, or publishing personal data.

10.2. If you come across a personal data breach, report to your Data Protection Officer.

11. Anonymised data preference

11.1. Do not use personal data unless it is strictly necessary for your task and proportionate to meeting the pre-defined purpose of your activity.

11.2. If anonymous data is not available, but personal data is, ensure that the data is anonymised before its further use, if possible.

11.3. Non-anonymised data should in no case be made public (or open data), unless strictly required for carrying out the task in question, and unless cleared by the Data Protection Officer for publication.

11.4. Where data is anonymised, do not proactively take any steps in the direction to re-identify the data (link the data to individual persons). The following techniques and procedures, for example, should be avoided unless the goal is actually to re-identify otherwise anonymous or pseudonymised data:

11.4.1. *Singling out*, which corresponds to the possibility to isolate some or all

records which identify an individual in the dataset;

11.4.2. *Linkability*, which is the ability to link, at least, two records concerning the same data
subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against “singling out” but not against linkability; or

11.4.3. *Inference*, which is the possibility to deduce, with significant probability, the value of
an attribute from the values of a set of other attributes.

11.5. If the risk of re-identification materializes on a given dataset, take all reasonable steps, seek appropriate expert advice and apply all relevant professional standards in order to mitigate the risk of a privacy breach and further unlawful personal data processing.

Annex B - preliminary privacy and ethics assessment of possible dataset combinations

Group	Variable Name	Details	Privacy impact?	Possible mitigator	Ethics impact?	Possible mitigator
Digital Twin	Building footprints		Unlikely	-	Unlikely	-
Digital Twin	3D city model	only Brabrand so far	Unlikely	-	Unlikely	-
Digital Twin	Orthophotos spring Webmercator	web mercator CRS for easier web integration	Unlikely	-	Unlikely	-
Digital Twin	Terrain and surface raw data	resolution 0.4m	Unlikely	-	Unlikely	-
Cross-sectoral: Environmental	weather data: temperature, wind, precipitation		Unlikely	-	Unlikely	-
Cross-sectoral: Social	Demographics: Population age distribution	on household level	Unlikely	-	Unlikely	-
Cross-sectoral: Social	Demographics: Population gender distribution	on household level	Unlikely	-	Unlikely	-
Cross-sectoral: Social	Demographics: Population ethnicity distribution	on household level	Unlikely as standalone. Possible linkability problem in combination with other data (e.g. detailed geospatial point and public land registry data) may be able to reveal ethnicity of (re-)identifiable individuals or specific households.	Aggregate front end display on a higher than single point level, e.g. street, cluster, section of the neighborhood.	Possible as standalone if LDT results portrayed with unfavorable connotations or LDT output can be used or misinterpreted to discriminate based on ethnicity. Exacerbated risk in combination with detailed geospatial points.	Clearly define LDT user epics and roles and BIPED purpose / objectives for the front end display to minimize risk of misinterpretation. Suggestion to aggregate display on higher than single geospatial point level.
Cross-sectoral: Environmental	Land Use pattern	on parcel level	Unlikely	-	Unlikely	-

Cross-sectoral: Environmental	green space		Unlikely	-		
Cross-sectoral: Environmental	air quality model	continuous spatial dataset covering the AOI	Unlikely	-	Unlikely. Hypothetical examples of remote impact may include downward pressure on real estate prices, but these are difficult to predict and control.	-
Cross-sectoral: Environmental	road network / segments	road segments input data for space syntax analysis (connectivity / accessibility	Unlikely	-		
Mobility	Road network		Unlikely	-	Unlikely	-
Mobility	Traffic generators (zones)		Unlikely	-		
Mobility	OD matrix	OD matrix connecting traffic generators and network	Unlikely	-	Unlikely	-
Mobility	Sensor traffic data		FCD is unlikely to cause any issue since the sensors are typically privacy-by-design solutions. ANPR in highly specific cases may create an inference problem. For example, unique number plate for hydrogen powered vehicles,	-	Unlikely. Hypothetical examples of remote impact may include downward pressure on real estate prices, but these are difficult to predict and control.	-
Mobility	Sensor data Calibration of traffic model		Unlikely	-	Unlikely	-
Cross-sectoral: Environmental	Noise measurements	on sensor level	Unlikely	-	Linkability problem if combined with highly specific geospatial points, may allow precise	Make harder to identify specific noise pollutants in the widely accessible LDT model.

					identification of noise pollutants / source of noise.	
Cross-sectoral: Environmental	Noise model	continuous spatial dataset covering the AOI	Unlikely	-	Linkability problem if combined with highly specific geospatial points, may allow precise identification of noise pollutants / source of noise.	Make harder to identify specific noise pollutants in the widely accessible LDT model.
Energy	Enriched Dataset on District heating from Kredsløb	Demand from individual buildings in Brabrand	Unlikely	-	Linkability problem: may allow identifying individual consumption patterns if combined with highly specific geospatial points (and publicly available land registry data).	-
Energy	Power Grid: Consumption data based on user		Unlikely	-	Linkability problem: may allow identifying individual consumption patterns if combined with highly specific geospatial point (and publicly available land registry data).	-
Energy	Power Grid: Dataset of substations		Unlikely	-	Unlikely	-
Energy	Power Grid: Aggregate consumption data on each building		Unlikely	-	Unlikely	-
Cross-sectoral: Environmental	Altitude model		Unlikely	-	Unlikely	-
Energy	District heating circuit and infrastructure	Location of district heating circuit lines and distribution system	Unlikely	-	Hypothetical concerns from a strategic/defense perspective if the LDT significantly enhances precision of the provided information.	These remote impacts may be difficult to estimate. In case of serious doubts, consult appropriate public authorities.

Energy	Energy infrastructure	Location of power infrastructure and distribution system	Unlikely	-	Hypothetical concerns from a strategic/defense perspective if the LDT significantly enhances precision of the provided information.	These remote impacts may be difficult to estimate. In case of serious doubts, consult appropriate public authorities.
Meteorological forecasts	Energy system	Standard MET forecasts	Unlikely	-	Unlikely	-
Cross-sectoral: Environmental	Identified infrastructure resilience options on energy systems		Unlikely	-	Unlikely	-