DIVAIRCITY

The power of Diversity & Inclusion for Climate Neutral Cities

Ethics, privacy and security data management requirements

Lead Beneficiary: Blockchain Intelligence

Disclaimer:

"This document has been prepared in the context of Divaircity project, funded by the EU Horizon 2020 research and innovation programme under the Grant Agreement No 101003799*. This document reflects only the authors' views and the Agency and the Commission are not responsible for any use that may be made of the information it contains."*

HISTORY OF CHANGES

Version	Date	Authors
V1.0	31/03/2022	Katharina Miller/Almudena de la Mata
V1.1	10/05/2022	Katharina Miller/ Almudena de la Mata
V1.2	17/05/2022	Katharina Miller/Almudena de la Mata
V1.3	31/05/2022	Elisa Peñalvo

LIST OF ACRONYMS

Acronym	Meaning
AB	Advisory Board
ALLEA	European Federation of Academies of Sciences and Humanities
CA	Consortium Agreement
CM	Consortium Members
DoA	Description of Actions
DMP	Data Management Plan
DPO	Data Protection Officer
EC	European Commission
EU	European Union
HRBAD	Human Rights-Based Approach to Data
IPR	Legal and Intellectual Property Rights
GA	Grant Agreement
GDPR	General Data Protection Regulation
SCCC	Smart Climate City Contract
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101003799

TABLE OF CONTENTS

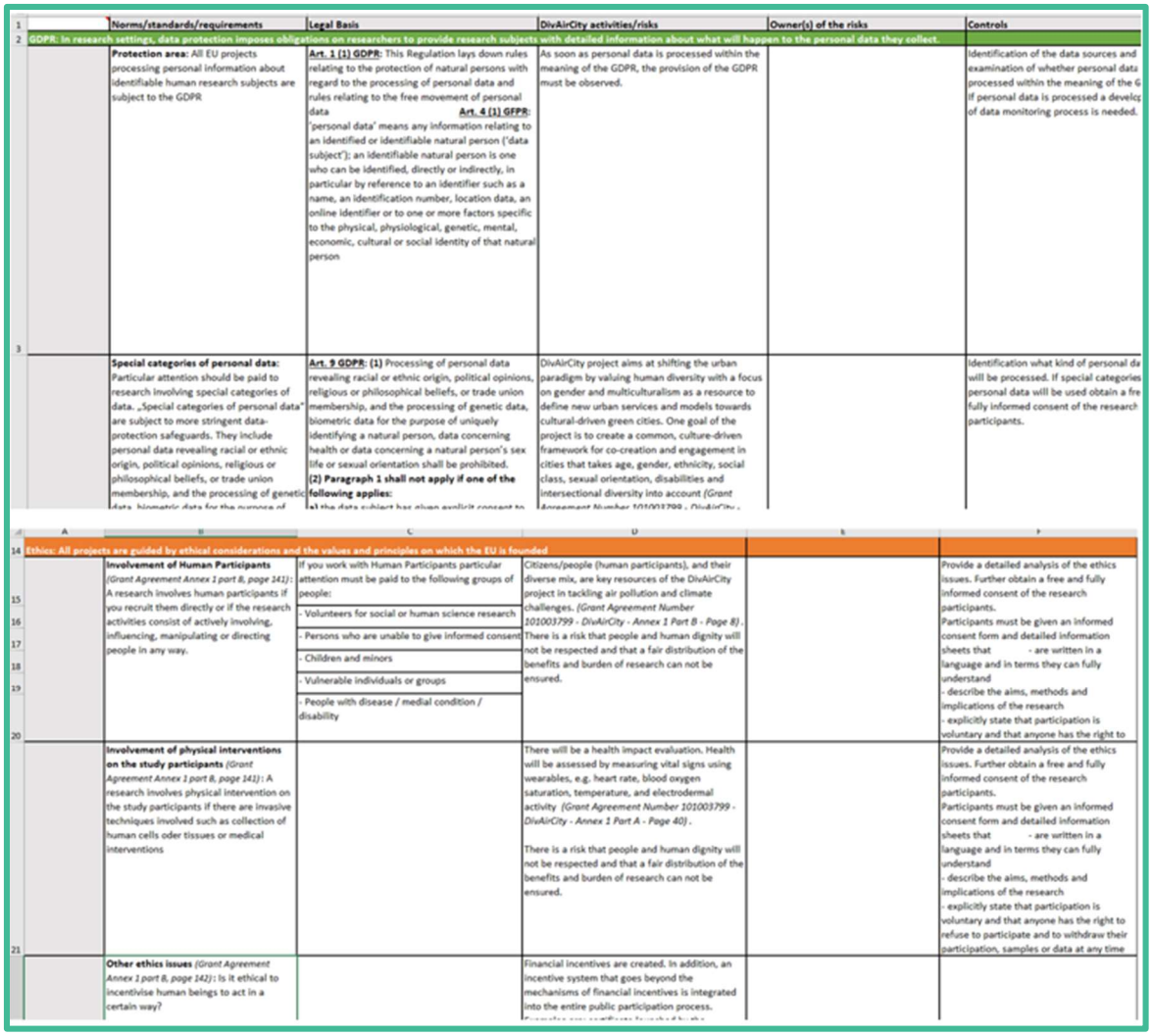
ABSTRACT

Deliverable 2.3 *Ethics, privacy and security data management requirements* includes a Framework, Guideline and operational tools for the implementation of the GDPR, legal and ethics related data management requirements at national and EU level. We stress the need to designate compliance and privacy officers and structures by every partner to ensure compliance with GDPR and further applicable legislation. The nature and volume of data managed within DivAirCity is particularly relevant and imply a high level of risk for privacy of the parties and citizens involved. The purpose of this deliverable is not to substitute the activities of designated responsible parties for GDPR compliance but to serve as a guide to all the participants and raise awareness on the importance of privacy and ethics in the specific sets of activities performed within the Project. It is of the upmost importance that the highest management of the organizations involved at DivAirCity are aware and assume the responsibility for the data that their organizations manages as it is subject to applicable legislation.

All three documents are to be used by DivAirCity partners who interact with citizens. These documents combine and complement each other and there is no hierarchy between them.

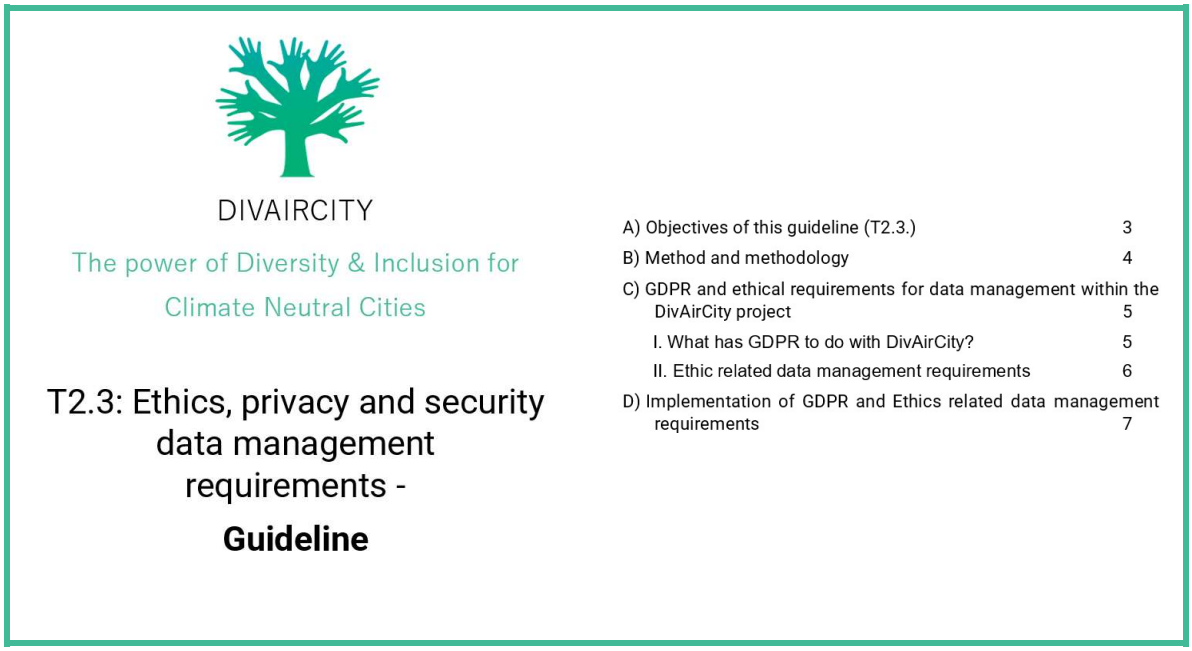
The **Framework (Figure 1)** provides a risk map of the GDPR and ethics related research activities planned within DivAirCity at the current standpoint. It is a document that can be used by all partners within DivAirCity that interact with citizens and that want to get an overview of GDPR and ethics related issues. The risks have been identified on the basis of the activities declared as planned by the partners through specific inquiries. Since DivAirCity is a living project, new activities might be conceived that are currently not identifiable and therefore, each partner should be responsible to include any new activity in their own risk map.

The **Guideline (Figure 2)** is an explanatory document to the Framework. Partners who interact with citizens can obtain detailed information on the GDPR and ethics related issues and they find guidance on how to tackle and address these issues.



	Norms/standards/requirements	Legal Basis	DivAirCity activities/risks	Owner(s) of the risks	Controls
GDPR: In research settings, data protection imposes obligations on researchers to provide research subjects with detailed information about what will happen to the personal data they collect.					
	Protection area: All EU projects processing personal information about identifiable human research subjects are subject to the GDPR	**Art. 1 (1) GDPR:** This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data **Art. 4 (1) GFPR:** 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	As soon as personal data is processed within the meaning of the GDPR, the provision of the GDPR must be observed.		Identification of the data sources and examination of whether personal data processed within the meaning of the G If personal data is processed a develo of data monitoring process is needed.
	Special categories of personal data: Particular attention should be paid to research involving special categories of data. „Special categories of personal data" are subject to more stringent data-protection safeguards. They include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic	**Art. 9 GDPR: (1)** Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. **(2) Paragraph 1 shall not apply if one of the following applies:**	DivAirCity project aims at shifting the urban paradigm by valuing human diversity with a focus on gender and multiculturalism as a resource to define new urban services and models towards cultural-driven green cities. One goal of the project is to create a common, culture-driven framework for co-creation and engagement in cities that takes age, gender, ethnicity, social class, sexual orientation, disabilities and intersectional diversity into account *(Grant*		Identification what kind of personal da will be processed. If special categories personal data will be used obtain a fre fully informed consent of the research participants.
Ethics: All projects are guided by ethical considerations and the values and principles on which the EU is founded					
	Involvement of Human Participants *(Grant Agreement Annex 1 part B, page 141)*: A research involves human participants if you recruit them directly or if the research activities consist of actively involving, influencing, manipulating or directing people in any way.	If you work with Human Participants particular attention must be paid to the following groups of people: - Volunteers for social or human science research - Persons who are unable to give informed consent - Children and minors - Vulnerable individuals or groups - People with disease / medial condition / disability	Citizens/people (human participants), and their diverse mix, are key resources of the DivAirCity project in tackling air pollution and climate challenges. *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part B - Page 8)*. There is a risk that people and human dignity will not be respected and that a fair distribution of the benefits and burden of research can not be ensured.		Provide a detailed analysis of the ethics issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that - are written in a language and in terms they can fully understand - describe the aims, methods and implications of the research - explicitly state that participation is voluntary and that anyone has the right to
	Involvement of physical interventions on the study participants *(Grant Agreement Annex 1 part B, page 141)*: A research involves physical intervention on the study participants if there are invasive techniques involved such as collection of human cells oder tissues or medical interventions		There will be a health impact evaluation. Health will be assessed by measuring vital signs using wearables, e.g. heart rate, blood oxygen saturation, temperature, and electrodermal activity *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 40)*. There is a risk that people and human dignity will not be respected and that a fair distribution of the benefits and burden of research can not be ensured.		Provide a detailed analysis of the ethics issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that - are written in a language and in terms they can fully understand - describe the aims, methods and implications of the research - explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time
	Other ethics issues *(Grant Agreement Annex 1 part B, page 142)*: Is it ethical to incentivise human beings to act in a certain way?		Financial incentives are created. In addition, an incentive system that goes beyond the mechanisms of financial incentives is integrated into the entire public participation process.		

Figure 1. Screenshot of the document "Building Block I Framework T2.3"



DIVAIRCITY

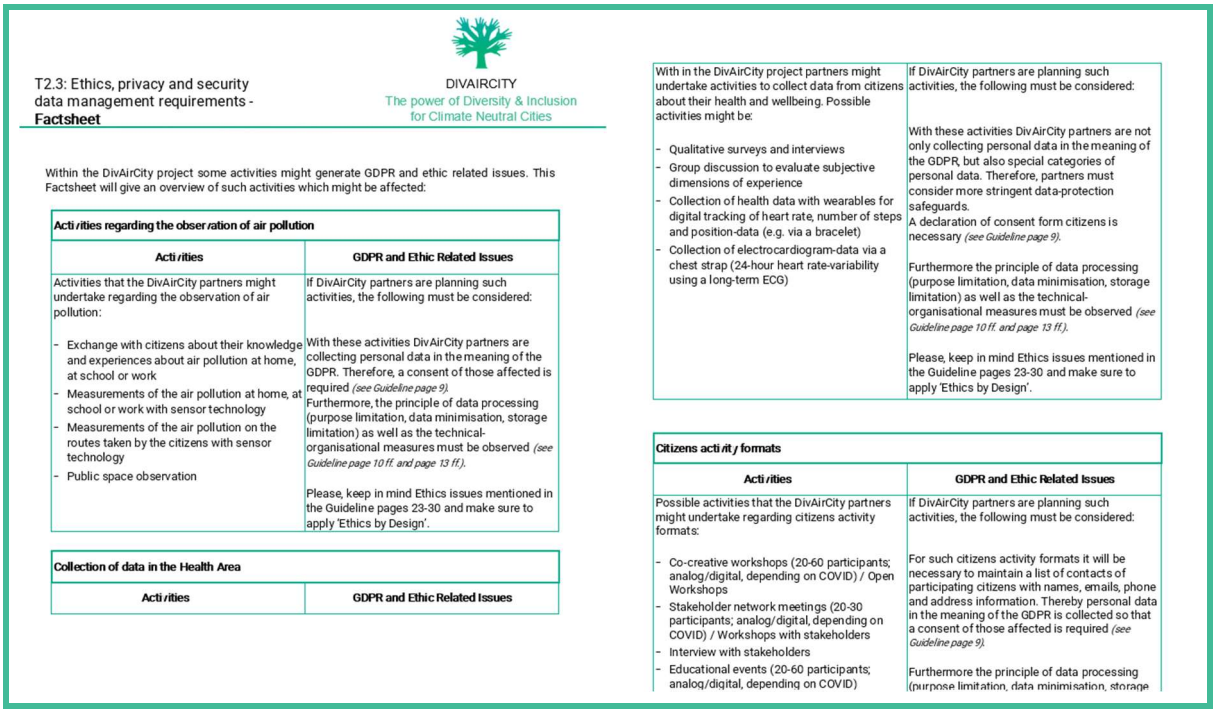
The power of Diversity & Inclusion for Climate Neutral Cities

T2.3: Ethics, privacy and security data management requirements -

Guideline

Figure 2. Screenshot of the document "Building Block II Framework T2.3"

The **operational tool (Figure 3)** is created as a Factsheet for partners within DivAirCity who interact with citizens and it gives a user-friendly overview on DivAirCity activities and their GDPR and ethics related issues, with reference back to the guideline for more detailed information.



T2.3: Ethics, privacy and security data management requirements - **Factsheet**

DIVAIRCITY
The power of Diversity & Inclusion for Climate Neutral Cities

Within the DivAirCity project some activities might generate GDPR and ethic related issues. This Factsheet will give an overview of such activities which might be affected:

Activities regarding the observation of air pollution

Activities	GDPR and Ethic Related Issues
Activities that the DivAirCity partners might undertake regarding the observation of air pollution: - Exchange with citizens about their knowledge and experiences about air pollution at home, at school or work - Measurements of the air pollution at home, at school or work with sensor technology - Measurements of the air pollution on the routes taken by the citizens with sensor technology - Public space observation	If DivAirCity partners are planning such activities, the following must be considered: With these activities DivAirCity partners are collecting personal data in the meaning of the GDPR. Therefore, a consent of those affected is required *(see Guideline page 9).* Furthermore, the principle of data processing (purpose limitation, data minimisation, storage limitation) as well as the technical-organisational measures must be observed *(see Guideline page 10 ff. and page 13 ff.).* Please, keep in mind Ethics issues mentioned in the Guideline pages 23-30 and make sure to apply 'Ethics by Design'.

Collection of data in the Health Area

Activities	GDPR and Ethic Related Issues
With in the DivAirCity project partners might undertake activities to collect data from citizens about their health and wellbeing. Possible activities might be: - Qualitative surveys and interviews - Group discussion to evaluate subjective dimensions of experience - Collection of health data with wearables for digital tracking of heart rate, number of steps and position-data (e.g. via a bracelet) - Collection of electrocardiogram-data via a chest strap (24-hour heart rate-variability using a long-term ECG)	If DivAirCity partners are planning such activities, the following must be considered: With these activities DivAirCity partners are not only collecting personal data in the meaning of the GDPR, but also special categories of personal data. Therefore, partners must consider more stringent data-protection safeguards. A declaration of consent form citizens is necessary *(see Guideline page 9).* Furthermore the principle of data processing (purpose limitation, data minimisation, storage limitation) as well as the technical-organisational measures must be observed *(see Guideline page 10 ff. and page 13 ff.).* Please, keep in mind Ethics issues mentioned in the Guideline pages 23-30 and make sure to apply 'Ethics by Design'.

Citizens activity formats

Activities	GDPR and Ethic Related Issues
Possible activities that the DivAirCity partners might undertake regarding citizens activity formats: - Co-creative workshops (20-60 participants; analog/digital, depending on COVID) / Open Workshops - Stakeholder network meetings (20-30 participants; analog/digital, depending on COVID) / Workshops with stakeholders - Interview with stakeholders - Educational events (20-60 participants; analog/digital, depending on COVID)	If DivAirCity partners are planning such activities, the following must be considered: For such citizens activity formats it will be necessary to maintain a list of contacts of participating citizens with names, emails, phone and address information. Thereby personal data in the meaning of the GDPR is collected so that a consent of those affected is required *(see Guideline page 9).* Furthermore the principle of data processing (purpose limitation, data minimisation, storage

Figure 3. Screenshot of the document "Building Block III Factsheet T2.3"

If a partner organises a DivAirCity event involving human participants they could use the Factsheet which gives an overview of the GDPR and ethics related issues. It is conceived as an easy-to-read document so that every person or organisation working in the activity can check on possible GDPR and ethical risks. The Factsheet refers to the Guideline for more information. The Guideline provides deeper knowledge while the Framework gives a technical risk map and legal and ethics references.

1 INTRODUCTION

1.1 Background of this Deliverable

D2.3 is the Deliverable of the DivAirCity Task 2.3 *Ethics, privacy and security data management requirements*. The Task is part of WP2 *Digital Innovation and D&I Data Management Framework* and is meant to contribute to identifying privacy, security and ethics measures in relation to data management of relevance for DivAirCity and to suggest mitigation strategies to the consortium.

It is important to stress that T2.3 and its Deliverable (D2.3) is focused on research activities in DivAirCity on European level. Accordingly, this task aims to identify GDPR and ethics related risks and facilitate a set of suggested related measures to DivAirCity research activities. Applicable legislation might evolve over the timeframe of the DivAirCity project. Actual compliance needs to be ensured by each of the partners considering EU, national and local legislation. DivAirCity as such does not have a Data Protection Officer and T2.3 does not deliver tailormade European or national legal advice to each DivAirCity partner. Furthermore, while DivAirCity partners have planned a large number of activities to fulfil the objectives of the project, these are likely not exhaustive of the actions to be performed until the end of the project. Consequently, the task does not address issues related to national impact on privacy and data protection, on discriminatory issues or on societal liberties in regard to the implementation of the DivAirCity technologies as part of an operational checkpoint. All partners have to make sure to comply with GDPR and their national legislations. This document does not tackle the question of the legal feasibility of implementing the DivAirCity risk-based concept, nor the issue of acceptance of the developed technologies among the general public. These questions are addressed in different tasks and deliverables.

1.2 Aim of the document

The purpose of this document is to report the development of the supporting material that has been developed in the first eight months of the DivAirCity project to advise the consortium on how to ensure the compliance with ethics, privacy and security data management requirements in the future. It focuses on the following issues:

- Data Protection (GDPR)
- Ethics.

It is important to stress that each partner will have a role regarding the data that will be managed and needs to be aware of their responsibility to be compliant with GDPR and their national legislations at any time and establish the necessary structures and roles to ensure full compliance. T2.3 cannot and will not deliver tailormade solutions or legal advice on national data protection or ethics issues.

The three documents complement each other and can be used independently. There is no hierarchy between them.

- The **Framework** provides a risk map on the GDPR and ethics related issues for the activities identified so far by all partners within DivAirCity who interact with citizens.
- The **Guideline** is an explanatory document to the Framework. In it, the partner who interacts with citizens can get information on the GDPR and ethics related issues and they get guidance on how to tackle and address these issues according to their own national legislations.
- The **Operational tool** is created as a Factsheet for partners within DivAirCity who interact with citizens and it gives an overview on planned DivAirCity activities and their GDPR and ethics related issues. The Factsheet serves as quick orientation tool, giving its readers the necessary input for further actions which are described in the Guideline. Hence, the Factsheet is referencing back to the Guideline.

1.3 Input / Output to this Document

Input to this Deliverable is the work across all WPs, WP1 and WP9 regarding the Data Management Plan and data manager officer appointment (D1.6); Ethical Board Member List (D1.9); Legal and Intellectual Property Rights (IPR) requirements report (D11); Requirement No. 2 (D9.1) and Requirement No. 3 (D9.2). Further important input is provided by the DivAirCity Grant Agreement. The Ethical Charter (D1.7) focuses on the internal DivAirCity structure and serves as Code of Conduct for and within the Consortium and its member organizations. It does not involve the ethical research aspects and or data management issues and that is why we do not refer to the Ethical Charter in this document. The output of this deliverable will provide ethics and GDPR related measures for research activities with citizens when involving humans and the use of personal data, as well as workshops and the pilots of DivAirCity. In terms of WPs, it will provide input across all WPs and especially the cities. Furthermore, the implementation of the Framework, Guideline and Operational tools in all DivAirCity deliverables related to research activities with citizens should be carried after May 2022.

2 METHODOLOGY

As mentioned above, the aim of Task 2.3 has been to develop a Framework, Guideline and Operational tools for the implementation of the GDPR, legal and ethics related data management requirements at a national and EU level, especially as an input for WP5 D&I SCCC.

At an early stage and as requested by DivAirCity partners, we decided to put emphasis on the 'operational' approach. This means that our intention has been to give practical, usable and therefore operational documents to DivAirCity partners that could support them in navigating their research with subjects and making them aware of the accompanying data management challenges. Therefore, our decision was to create a Framework with an Excel document to signal all risks (a streamlined risk map). The idea is to have an integrated Framework for managing DivAirCity risks related to data management by analysing threats across DivAirCity, work packages and activity levels, and suggesting controls (Dey, 2010). The guideline is an accompanying word document to the framework, giving information on the risks, the risk owners and suggestions on how to prevent or mitigate them. The operational tool is created as a Factsheet: a short document that contains the most relevant information about a the DivAirCity data management risks in only three pages (Cubon-Bell, 2019).

As mentioned before there are several overlaps with other WPs, such as WP1 and WP9 regarding the *Data Management Plan and data manager officer appointment* (D1.6), *Ethical Board Member List* (D1.9), *Legal and Intellectual Property Rights* (IPR) requirements report (D.11), Requirement No. 2 (D9.1) and Requirement No. 3 (D9.2). Therefore, the general approach of T2.3 has been to cooperate with these two WPs.
In addition, desk research such as literature review and legal text interpretation method of GDPR and other legal related data management requirements at EU level have been performed:

- European Commission (2018), *Ethics and data protection*, 14 November 2018.
- European Commission (2018), *Ethics in Social Science and Humanities,* October 2018.
- European Agency for Cybersecurity (ENISA), *Deploying Pseudonymisation Techniques*, 2022.
- Horizon 2020 Framework Programme of the European Union, GDPR.eu, https://gdpr.eu/

- Information Commissioner's Office, *Determining what is personal data*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
- *Regulation (EU) 2016/679 of the European Parliament and of the Council* of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing *Directive 95/46/EC* (General Data Protection Regulation) (Text with EEA relevance)
- United Nations Development Programme (UNDP), *Data Futures Platform, 8 Data Principles for UNDP*, https://data.undp.org/data-principles/
- United Nations Development Group (2017), *Data Privacy, Ethics and Protection, Guidance note on big data for achievement of the 2030 Agenda.*

On a national level, partners will have to refer to their Data Protection Officers or similar.

Focus has been given to the relevant literature with a practical approach. In particular the following documents have been reviewed:

- ALLEA, *The European Code of Conduct of Research Integrity*, 2017.
- European Commission (2019), Horizon 2020 Programme, Guidance. *How to complete your ethics self-assessment, 4*. February 2019.
- Farkas, L (2017), *Data collection in the field of ethnicity. Analysis and comparative review of equality data collection practices in the European Union*, Directorate-General for Justice and Consumer, European Commission, 2017.
- United Nations Humans Rights, Office of the High Commissioner (2018), *A Human Rights-based approach to data. Leaving no one behind in the 2030 Agenda for Sustainable Development*, 2018.
- Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. *The FAIR Guiding Principles for scientific data management and stewardship*. Sci Data 3, 160018 (2016). https://doi.org/10.1038/sdata.2016.18

An ethics text interpretation method (Knottnerus and Tugwell, 2018) and analysis of the activities planned within DivAirCity leads to the ethics requirements (see D9.2) and identification of ethics issues.

In order to link the ethics related data management requirements with the DivAirCity related activities, especially those of the activities of the five cities themselves and WP5 D&I SCCC, an inquiry set of activities with all the related partners were performed. Specific meeting sessions have taken place with DivAirCity partners. Feedback has been also requested to the partners in written form. Throughout the inquiry period DivAirCity partners who interact with citizens (or plan to do so) explained their upcoming activities. This information has been integrated into the Guideline and the Factsheet *(see **Annex I**)*. However, in these first 8 months, not all partners had yet a clear view of their full set of possible future activities involving research subjects and therefore having to focus on data management challenges. This had an impact on our planning and development for the Framework, Guideline and Factsheet and it obliged us to draft these three documents under a high-level approach so that all partners can work with these documents in the coming years.

For all three documents, the Framework, the Guideline and the Factsheet, we applied the risk analysis method (Abie and Borking, 2012). This method is used during the planning of information to identify security requirements as, in this case, the GDPR and ethics requirements.

3 Ethics of data management

Even though the aim of this document is to report the development of the supporting material that has been developed in the first eight months of the DivAirCity project, a short overview on how ethics of data management is important for DivAirCity researchers shall be given. As stated above, the nature of the data – i.e., health or data revealing ethical and racial origin — and volume of data managed within DivAirCity is particularly relevant and imply a high level of risk for privacy and human rights of the research participants involved.

Ethics of data management in research is not an isolated and linear process of merely 'putting data under control'. This is for example the case with the legal obligations to comply with GDPR. Instead, within ethics of data management in research 'data flows in multiple directions and interacts with a variety of actors throughout and beyond the research process' (Tang).

Inspired by Tang's *Ecology of Data Management*, we suggest the following *Life cycle of data management of DivAirCity*:

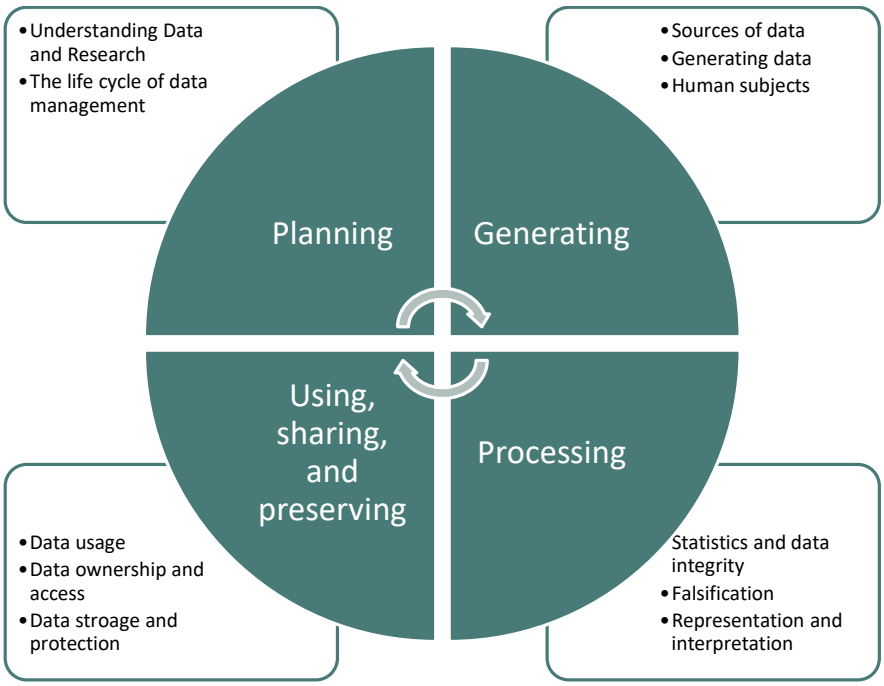


Figure 4. The Life cycle of data management of DivAirCity

As can be observed in Figure 4, this life cycle of data management includes four processes: planning, generating, processing and using, sharing and preserving. All four processes can be case sites for ethics issues for DivAirCity researchers, and this shall

be explained in the following. According to the European Charter for Researchers[1], researchers should focus on the good of humankind and always according to **recognized principles** and practices. The United Nations Human Rights Office of the High Commissioner has elaborated a **set of principles for a Human Rights-Based Approach to Data** (HRBAD)[2]. These principles include participation, data disaggregation, self-identification, transparency, and accountability.

The **first principle is participation**. According to HRBAD, 'participation of relevant population groups in data collection exercises, including planning, data collection, dissemination and analysis of data'[3] is crucial. In the *Life cycle of data management of DivAirCity* this principle affects the processes planning and generating. DivAirCity researchers have to understand data and research even though some population groups may seem distant to them — such as for example marginalised groups — and they must include human subjects and generate data by relevant population groups. According to HRBAD, the participation can be achieved by:

- Considering a range of processes that facilitate and encourage participation of relevant population groups.
- Clearly communicating on the participatory processes and the outcomes of the exchanges to human subjects.
- Including views of vulnerable or marginalised groups, and those who are at risk of discrimination.

The **second HRBAD principle is data disaggregation**. Disaggregated data is data that has been broken down by categories, for example by vulnerable or marginalised groups, sex or gender, ethnical or racial origin. Disaggregated data can reveal inequalities and deprivations that may not be fully reflected in aggregated data[4]. This principle affects the life cycle's processes planning, generating and processing. Researchers have to integrate different categories in their research framework

[1] The European Charter for Researchers (2000), in https://euraxess.ec.europa.eu/jobs/charter/european-charter (last access on 16.05.2022).
[2] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data.
[3] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data, page 3.
[4] UN Women (2021), Counted and Visible: Toolkit to better utilize existing data from household surveys to generate disaggregated gender statistics, in https://unstats.un.org/unsd/statcom/52nd-session/documents/BG-3l-Executive_Summary_Counted_and_Visible_Toolkit-E.pdf, page 4 (last access on 16.05.2022).

(Planning process), they have to generate the different categories of data and do a correct interpretation to reveal to possible inequalities and deprivations. According to HRBAD, this can be adequately realised by:

- Generating more detailed data than national averages. This is key in identifying and understanding inequalities.
- Disaggregating data according to characteristics identified in international human rights law.
- Establishing alternate sampling and data collection approaches.

The **third HRBAD principle is self-identification.** According to HRBAD, 'for the purposes of data collection, populations of interest should be self-defining. Individuals should have the option to disclose, or withhold information about their personal characteristics'[5]. The principle affects especially the process 'generating' within the life cycle. DivAirCity researchers will have to carefully listen to the human subjects and how they want to define themselves. This should also be foreseen in the 'planning' process within the life cycle. According to HRBAD, the principle of self-identification can be respected by:

- It should be at the individual's discretion how and which data about their personal characteristics they want to provide.
- Data collection activities should be conducted in accordance with the human rights principle of 'doing no harm'.

Another **HRBAD principle is transparency**. According to HRBAD, 'data collectors should provide clear, openly accessible information about their operations, including research design and data collection methodology. Data collected by State agencies should be openly accessible to the public'[6]. This principle affects especially the processes processing and using, sharing and preserving within the life cycle. DivAirCity researchers and especially the cities should act with data integrity and don't falsify any data; they should furthermore make their data usage public and give access to the public. This is also in line with the FAIR principles (Findable, Accessible, Interoperable

[5] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data, page 11.
[6] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data, page 14.

and Re-usable) for data management[7]. According to HRBAD, this principle of transparency can be fulfilled by:

- Making information about data collection publicly available.
- Disseminating of data as quickly as possible after its collection.

The last HRBAD principle that we discuss is **accountability**. According to HRBAD, 'data collectors are accountable for upholding human rights in their operations, and data should be used to hold States and other actors to account on human rights issues'. This principle affects the whole *Life cycle of data management of DivAirCity*, because researchers, especially the cities as duty-bearers, are accountable for respecting, protecting and fulfilling human rights of the research subjects at all times of the four processes. One important document that can assure DivAirCity researchers' accountability is the *ALLEA European Code of Conduct for Research Integrity*[8]. DivAirCity researchers should base their research on the following four principles of the *ALLEA European Code of Conduct for Research Integrity*:

- 'Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.
- Respect for colleagues, research participants, society, ecosystems, cultural heritage and the environment.
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.'[9]

The above shows that ethics in data management is not a schematic process; it is rather an ongoing process, a 'life cycle', in which researchers have to question their activities from the very first moment on, when they start thinking and drafting their research processes. Helpful tools for researchers can be the presented HRBAD principles as well as the *ALLEA Code of Conduct of Research Integrity.*

---

[7] Wilkinson, M., Dumontier, M., Aalbersberg, I. *et al.* The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data* **3,** 160018 (2016). https://doi.org/10.1038/sdata.2016.18 2017 (last access on 16.05.2022).

[8] ALLEA, The European Code of Coduct for Research Integrity, in: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf (last access on 16.05.2022).

[9] See above, page 4 (last access on 16.05.2022).

4 DEVELOPMENT OF THE FRAMEWORK, GUIDELINE AND FACTSHEET

4.1 Framework

It was first agreed to draft a framework as a risk map of the planned DivAirCity activities. Therefore, it was necessary to identify the relevant GDPR and ethics issues regarding the DivAirCity project.

For the **identification of the GDPR topics,** we used the legal text of the GDPR[10] as well as the Ethics Requirements No. 3 from WP9. Although these are GDPR related issues, the European Commission treats them as Ethics issues or Ethics Requirements. As per Ethics Requirement No. 3[11], DivAirCity is obliged to focus on the following data protection issues:

- The beneficiary must explain how all the data intended to be processed is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation' principle).
- Description of the anonymisation/pseudonymisation techniques.
- Detailed information on the informed consent procedures regarding data processing.
- Templates of the informed consent forms and information sheets (in language and terms intelligible to the participants).
- In case the research involves profiling, the beneficiary must provide explanation how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded.
- In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects.

Out of these sources we worked out eleven issues regarding GDPR, that the partners who work with personal data of citizens can come across. These topics are:

1. **Protection Area of the GDPR**: All EU projects processing personal information about identifiable human research subjects are subjected to the GDPR.

[10] GDPR.EU: https://gdpr.eu/what-is-gdpr/ (last access on 10.02.2022).
[11] Grant Agreement Annex 1 part A, page 19.

2. **Special categories of personal data**: Particular attention should be paid to research involving special categories of data. 'Special categories of personal data' are subject to more stringent data-protection safeguards. They include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
3. **Profiling**: In case the research involves profiling, the beneficiary must provide explanation how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded. (Grant Agreement Annex 1 part A, page 53)
4. **Enlightenment/informed consent**: Obligation on researchers to provide research subjects with detailed information about what will happen to the personal data that they collect. This requires consent to be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the subjects' agreement to the processing of their personal data. As a minimum, this should include:
   a) the identity of the data controller
   b) the specific purpose of the processing
   c) information as to whether data will be shared with or transferred to third parties and for what purpose
   d) how long the data will be retained before they are destroyed
   The data subject must also be made aware if data is to be used for any other purposes, shared with research partners or transferred to organizations outside the EU and research subjects have to consent.
5. **Purpose limitation, data minimisation and storage limitation**: A data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. The data controller should also retain the data only for as long as is necessary to fulfil that purpose.
6. **Anonymisation/pseudonymisation of personal data**: Anonymise personal data so that they no longer relate to identifiable individuals. Data that no longer relate to identifiable persons, such as statistical data, are not personal data and are therefore outside the scope of data protection law.
7. **Processing of previously collected personal data (secondary use)**: In case of further processing of previously collected personal data, an explicit

confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects must be submitted as a deliverable previous to taking action (Grant Agreement Annex 1 part A, page 53).

8. **The 'Right to be Forgotten'**: Individuals have the right to request the data controller to delete their personal data as foreseen in Art. 17 GDPR.
9. **Data protection/privacy by design**: When planning a processing system, technical and organisational measures must be taken to ensure data security. Consequently, the term 'privacy by design' means data protection through technology design. Data protection can best be observed in data processing operations if it is already technically integrated during structural design.
10. **Data security**: Protect personal data against loss or misuse. The GDPR requires all data controllers and processors to implement appropriate technical and organisational measures to ensure a level of data security that is commensurate to the risks faced by the data subjects in the event of unauthorised access, disclosure, accidental deletion or destruction of their data.
11. **Designation of a data protection officer**.

This analysis is exhaustive, however we cannot exclude the possibility that there might be GDPR provisions that we have not included. Therefore, we cannot take responsibility for not having introduced some references to articles mentioned in D2.3 and the four annexes.

For the **identification** of the relevant **ethics related data management requirements** that the project must comply with, we have worked with the Ethics and data protection[12] guideline of the European Commission as well as with the Horizon 2020 Programme Guidance[13] of the European Commission. Furthermore, we incorporated the Ethics Requirements No. 2 from WP9[14]. According to the Ethics issues checklist of the Horizon 2020 Programme Guidance we have detected and included the following ethics issues:

[12] Ethics and data protection. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf (last access on 11.02.2022)
[13] Horizon 2020 Programme Guideance - How to complete your ethics self - assessment. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pd (last access on 11.02.20222)
[14] Grant Agreement Annex 1 part A, page 53.

1. Involvement of Human Participants: A research involves human participants if you recruit them directly or if the research activities consist of actively involving, influencing, manipulating or directing people in any way (see Ethics issues checklist).
2. Involvement of physical interventions on the study participants: A research involves physical intervention on the study participants if there are invasive techniques involved such as collection of human cells or tissues or medical interventions (see Ethics issues checklist).
3. Other ethic issues (see Ethics issues checklist).

After the identification of the requirements, the Framework was created in the form of an Excel spreadsheet, which is attached as **Building Block I**. Its aim is to show the partners of the DivAirCity Project what they need to be aware of regarding the implementation of the GDPR and ethics related data management requirements and issues. The framework was repeatedly adapted and revised during the development of the guideline. The aim was to adapt the Framework and Guideline so that they complemented each other at all times.

The following section refers to the Framework structure Excel, which can be found separate to this document as **Building Block I**.

Lines 4 to 15 concern **GDPR related issues**:

		Norms/standards/requirements	Legal Basis	DivAirCity activities/risks	Owner(s) of the risks	Controls
2	GDPR: In research settings, data protection imposes obligations on researchers to provide research subjects with detailed information about what will happen to the personal data they collect.					
3		**Protection area:** All EU projects processing personal information about identifiable human research subjects are subject to the GDPR	**Art. 1 (1) GDPR:** This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data **Art. 4 (1) GFPR:** 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	As soon as personal data is processed within the meaning of the GDPR, the provision of the GDPR must be observed.		Identification of the data sources and examination of whether personal data is processed within the meaning of the GD If personal data is processed a developm of data monitoring process is needed.
		Special categories of personal data: Particular attention should be paid to research involving special categories of data. „Special categories of personal data" are subject to more stringent data-protection safeguards. They include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic	**Art. 9 GDPR: (1)** Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. **(2) Paragraph 1 shall not apply if one of the following applies:**	DivAirCity project aims at shifting the urban paradigm by valuing human diversity with a focus on gender and multiculturalism as a resource to define new urban services and models towards cultural-driven green cities. One goal of the project is to create a common, culture-driven framework for co-creation and engagement in cities that takes age, gender, ethnicity, social class, sexual orientation, disabilities and intersectional diversity into account *(Grant*		Identification what kind of personal data will be processed. If special categories o personal data will be used obtain a free fully informed consent of the research participants.

Figure 5. Extract from the document "Building Block I Framework T2.3"

Column B shows the requirements which the GDPR stipulates and column C shows the corresponding legal basis. In column D, the activities of the DivAirCity Project should be displayed in order to work out possible risks of violating the norms mentioned in column C. The owner of the risk should be stated in column F. Finally, possible control mechanisms are recorded in column G in order to minimise the risk of a violation of the norms named in column C.

Lines 17 to 24 concern the **Ethic Requirements**:

	A	B	C	D	E	F
14	**Ethics: All projects are guided by ethical considerations and the values and principles on which the EU is founded**					
15		**Involvement of Human Participants** *(Grant Agreement Annex 1 part B, page 141)*: A research involves human participants if you recruit them directly or if the research activities consist of actively involving, influencing, manipulating or directing people in any way.	If you work with Human Participants particular attention must be paid to the following groups of people:	Citizens/people (human participants), and their diverse mix, are key resources of the DivAirCity project in tackling air pollution and climate challenges. *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part B - Page 8)*. There is a risk that people and human dignity will not be respected and that a fair distribution of the benefits and burden of research can not be ensured.		Provide a detailed analysis of the ethics issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that - are written in a language and in terms they can fully understand - describe the aims, methods and implications of the research - explicitly state that participation is voluntary and that anyone has the right to
16			- Volunteers for social or human science research			
17			- Persons who are unable to give informed consent			
18			- Children and minors			
19			- Vulnerable individuals or groups			
20			- People with disease / medial condition / disability			
21		**Involvement of physical interventions on the study participants** *(Grant Agreement Annex 1 part B, page 141)*: A research involves physical intervention on the study participants if there are invasive techniques involved such as collection of human cells oder tissues or medical interventions		There will be a health impact evaluation. Health will be assessed by measuring vital signs using wearables, e.g. heart rate, blood oxygen saturation, temperature, and electrodermal activity *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 40)*. There is a risk that people and human dignity will not be respected and that a fair distribution of the benefits and burden of research can not be ensured.		Provide a detailed analysis of the ethics issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that - are written in a language and in terms they can fully understand - describe the aims, methods and implications of the research - explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time
		Other ethics issues *(Grant Agreement Annex 1 part B, page 142)*: Is it ethical to incentivise human beings to act in a certain way?		Financial incentives are created. In addition, an incentive system that goes beyond the mechanisms of financial incentives is integrated into the entire public participation process.		

Figure 6. Extract from the document "Building Block I Framework T2.3"

Column B shows which involvements in the project may hold higher ethical risks. Column C / Line 17-22 identifies particularly vulnerable groups that need to be considered when involving human participants. In column D, the activities of the project are displayed that constitute a risk for the participations named in column C. The owner of the risk should be stated in column F. Possible control mechanisms are recorded in column G in order to minimize the risk of a violation of the ethical requirements.

4.2 Guideline

After completing the Framework, we included its content as continuous text in the Guideline, which is attached to this document as **Building Block II**. We stress the need to designate GDPR experts and structures which assume responsibility for compliance by every partner. The purpose of this Deliverable is not to substitute the activities of designated responsible parties for GDPR compliance but to serve as a guide to all the participants.

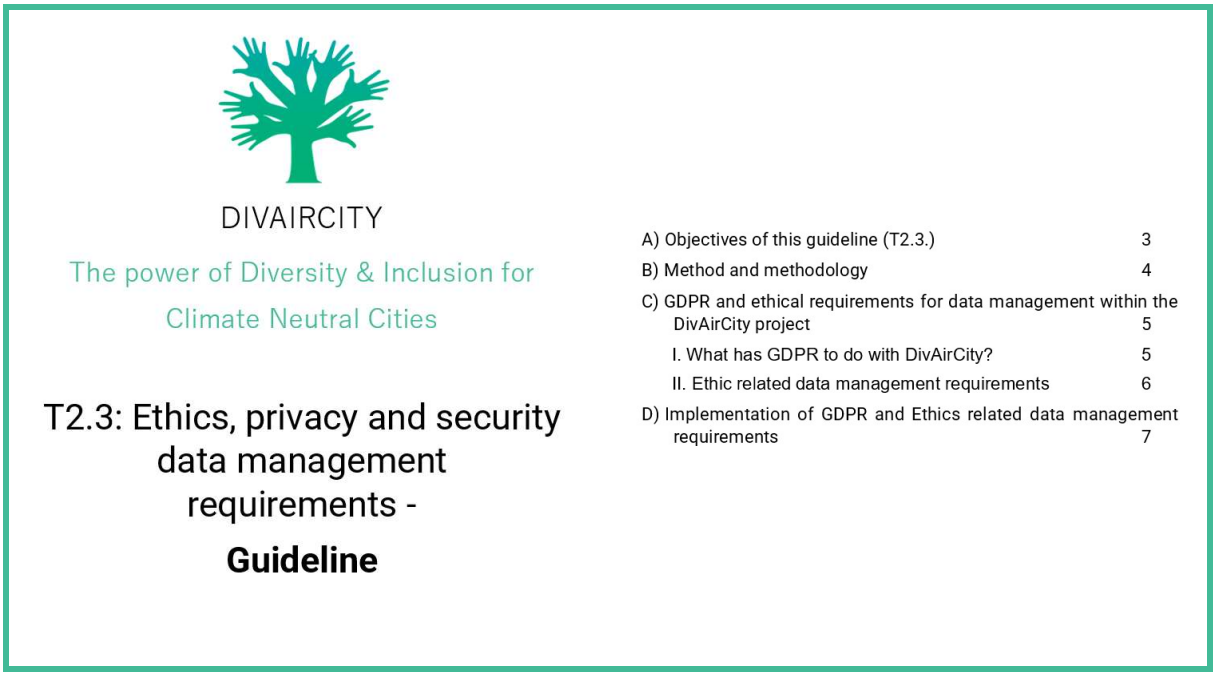
Hence, the Guideline has been conceived as a facilitator and enhancer of awareness to all the individuals involved in the project according to the activities actually identified so far. Language is therefore not technical and legal references have been avoided.

It is important to stress that the work of this deliverable has been based on the activities identified at the moment this report has been issued. Further actions might take place during the performance of the project and all the GDPR and ethical related questions must be dealt with by the partners' GDPR designated structures.

In order to capture all possible GDPR and Ethics related issues the data related activities that are already planned in WP2 were identified in cooperation with WP2 partners as well as the cities. For this purpose, the following activities where performed:

a) Awareness training on GDPR risks and ethical requirements of the DivAirCity project
b) Request for input was sent to all WP2 partners and the cities
c) A virtual meeting was held on the 1st of March 2022 with the objective of raising awareness, explaining the content of the deliverable and obtaining relevant input on the activities planned and the risks linked to them. With the input collected from the partners *(see **Annex I**)*, the first draft Guideline was finalised and shared with the partners from WP2.
d) Partners were asked to comment on the draft Guideline regarding their planned activities. Cities were also specifically addressed and requested to provide input on the activities they plan to organise which involve citizens participation and therefore also data management. Input was received from EcoWise, UPV, HPI, SIP, CNR, Potsdam, Aarhus, Castellon and collected the feedback in an Excel spreadsheet *(see **Annex I**)*.
e) The input and Feedback were integrated into the Guideline.

The Guideline is structured in four main parts which can found in figure 7.


DIVAIRCITY

The power of Diversity & Inclusion for Climate Neutral Cities

T2.3: Ethics, privacy and security data management requirements -

Guideline

Figure 7. Extract from the document "Building Block II Framework T2.3"

The objectives of the Guideline are described (A).

In the second part the method and methodology of the Guideline is presented (B).

Under section C, the GDPR and ethical requirements for data management within the DivAirCity project are stated under the understanding that it does not substitute the legal and compliance analysis by designated experts.

In the last part (D) the implementation of GDPR and Ethics related data management requirements are explained.

Part D) of the Guideline has the same structure as the Framework (see above). The purpose is that the partners of the DivAirCity project can get a general idea of GDPR and Ethics related issues in the Framework. In case they need further explanation, they can then read more about it in the Guideline.

The **first section of Part D)** is dedicated to the **GDPR requirements**, namely:

Protection Area of the GDPR

a. Special categories of personal data
b. Profiling
c. Enlightenment / informed consent
d. Purpose limitation, Data minimisation and storage limitation

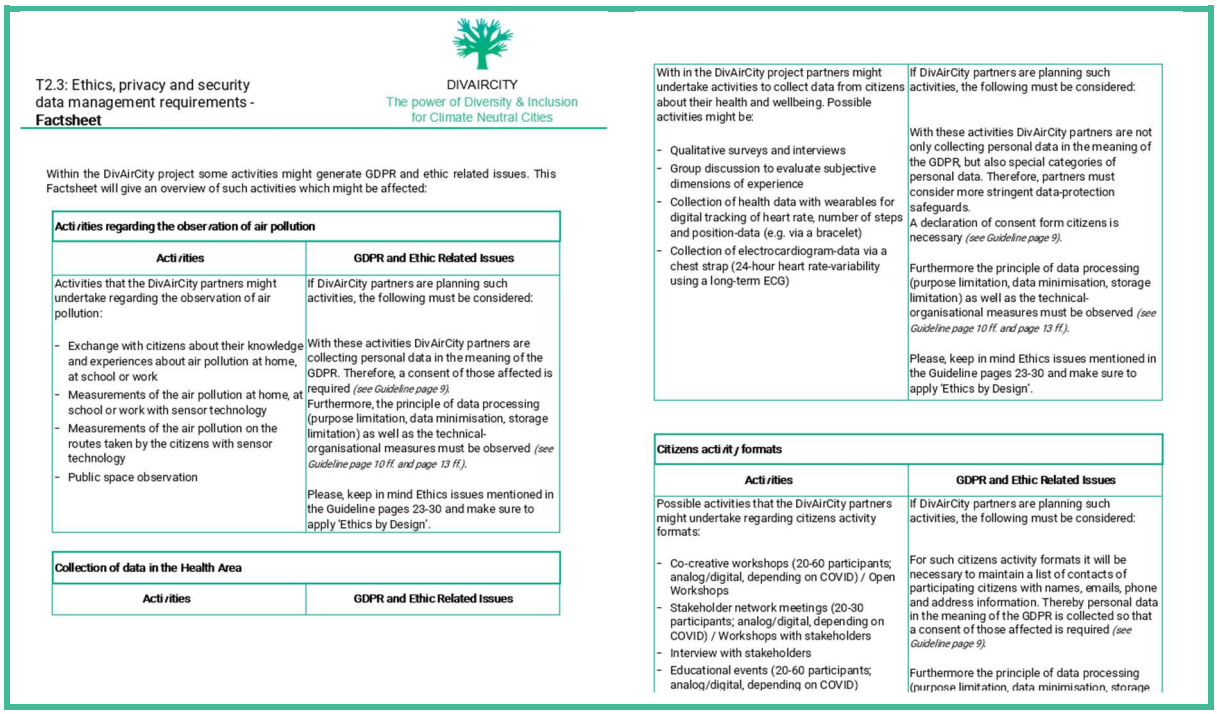
e. Anonymisation / pseudonymisation of personal data
f. Processing of previously collected personal data (secondary use)
g. The 'Right to be Forgotten'
h. Data protection / privacy by design
i. Data Security
j. Designation of a data protection officer

Within these requirements there is always a short introduction and explanation that aims to clarify what is presupposed by the GDPR, according to the *Ethics and data protection guideline* by European Commission. After the explanation of the DivAirCity activities / risks, the owner of the risk and the possible controls are stated. As mentioned above, this analysis is – to our best knowledge — exhaustive however we cannot exclude the possibility that there might be GDPR provisions that we have not included (i.e., due to the lack of information on DivAirCity activities, etc.). Therefore, we cannot take any responsibility for not having introduced some references to GDPR articles in D2.3, Annex I and Building Blocks I-III.

As in the Framework the **second section of Part D)** in the Guideline is addressed to the **Ethics related requirements or Ethics issues**.

4.3 Factsheet (=operational tool)

With the outcome of the Guideline and with the feedback of the DivAirCity partners we created a Factsheet (**Building Block III**), which gives partners *ad-hoc* information about their highest risks related to GDPR and ethics, when planning or conducting activities with citizens. This is deemed to create a broader awareness by all the personnel involved in personal data related to the project and in any case should it substitute the task of the designated compliance or data protection officers.



T2.3: Ethics, privacy and security data management requirements - Factsheet

DIVAIRCITY
The power of Diversity & Inclusion for Climate Neutral Cities

Within the DivAirCity project some activities might generate GDPR and ethic related issues. This Factsheet will give an overview of such activities which might be affected:

Activities regarding the observation of air pollution

Activities	GDPR and Ethic Related Issues
Activities that the DivAirCity partners might undertake regarding the observation of air pollution: - Exchange with citizens about their knowledge and experiences about air pollution at home, at school or work - Measurements of the air pollution at home, at school or work with sensor technology - Measurements of the air pollution on the routes taken by the citizens with sensor technology - Public space observation	If DivAirCity partners are planning such activities, the following must be considered: With these activities DivAirCity partners are collecting personal data in the meaning of the GDPR. Therefore, a consent of those affected is required *(see Guideline page 9).* Furthermore, the principle of data processing (purpose limitation, data minimisation, storage limitation) as well as the technical-organisational measures must be observed *(see Guideline page 10 ff. and page 13 ff.).* Please, keep in mind Ethics issues mentioned in the Guideline pages 23-30 and make sure to apply 'Ethics by Design'.

Collection of data in the Health Area

Activities	GDPR and Ethic Related Issues
With in the DivAirCity project partners might undertake activities to collect data from citizens about their health and wellbeing. Possible activities might be: - Qualitative surveys and interviews - Group discussion to evaluate subjective dimensions of experience - Collection of health data with wearables for digital tracking of heart rate, number of steps and position-data (e.g. via a bracelet) - Collection of electrocardiogram-data via a chest strap (24-hour heart rate-variability using a long-term ECG)	If DivAirCity partners are planning such activities, the following must be considered: With these activities DivAirCity partners are not only collecting personal data in the meaning of the GDPR, but also special categories of personal data. Therefore, partners must consider more stringent data-protection safeguards. A declaration of consent form citizens is necessary *(see Guideline page 9).* Furthermore the principle of data processing (purpose limitation, data minimisation, storage limitation) as well as the technical-organisational measures must be observed *(see Guideline page 10 ff. and page 13 ff.).* Please, keep in mind Ethics issues mentioned in the Guideline pages 23-30 and make sure to apply 'Ethics by Design'.

Citizens activity formats

Activities	GDPR and Ethic Related Issues
Possible activities that the DivAirCity partners might undertake regarding citizens activity formats: - Co-creative workshops (20-60 participants; analog/digital, depending on COVID) / Open Workshops - Stakeholder network meetings (20-30 participants; analog/digital, depending on COVID) / Workshops with stakeholders - Interview with stakeholders - Educational events (20-60 participants; analog/digital, depending on COVID)	If DivAirCity partners are planning such activities, the following must be considered: For such citizens activity formats it will be necessary to maintain a list of contacts of participating citizens with names, emails, phone and address information. Thereby personal data in the meaning of the GDPR is collected so that a consent of those affected is required *(see Guideline page 9).* Furthermore the principle of data processing (purpose limitation, data minimisation, storage

Figure 8. Extract from the document "Building Block III Framework T2.3"

Identified categories of data related activities

Due to the previous collected feedback from the partners, we were able to identify three different groups of possible activities that might take place in the future.

The first group contains **activities regarding the observation of air pollution**. Partners named the following possible activities *(*see also **Annex I**):

- Exchange with citizens about their knowledge and experiences about air pollution at home, at school or work
- Measurements of the air pollution at home, at school or work with sensor technology
- Measurements of the air pollution on the routes taken by the citizens with sensor technology
- Public space observation

The second group refers to **activities where data from citizens in the area of health might be collected**. Regarding the feedback possible activities are:

- Qualitative surveys and interviews
- Group discussion to evaluate subjective dimensions of experience

- Collection of health data with wearables for digital tracking of heart rate, number of steps and position-data (e.g., via a bracelet)
- Collection of electrocardiogram-data via a chest strap (24-hour heart rate-variability using a long-term ECG)

The third group covers **citizens activity formats** like:

- Co-creative Workshops (20-60 participants; analogue/digital, depending on COVID) / Open workshops
- Stakeholder network meetings (20-30 participants; analogue/digital, depending on COVID) / Workshops with stakeholders
- Interview with stakeholders
- Educational events (20-60 participants; analogue/digital, depending on COVID)
- Experimental workshops (small groups) / citizens science activities
- Contests
- Meet-ups

The Factsheet consists of a word document, that contains three tables. Each table includes one activity group. Furthermore, the tables are divided into one column for possible activities and one column for GDPR and Ethic related issues that might come up when conducting the described activities. The column for GDPR and Ethic related issues gives partners an overview of what they need to be aware and where they can get information within the guideline. In any case, they should inform their designated compliance or Privacy officer of any activity related to personal data and request guidance as to the activities necessary to be GDPR compliant. As mentioned above, this analysis is exhaustive, however we cannot exclude that there might be GDPR provisions that we have not included. Therefore, we cannot take responsibility for not having introduced some references to GDPR articles mentioned in D2.3 in the four building blocks.

5 References

[1] ALLEA, The European Code of Conduct of Research Integrity, 2017.

[2] Cubon-Bell, V. (2019). Teaching – Fact Sheets. Kent State University Center for Teaching and Learning. Retrieved on 12.05.2022 from Fact Sheets | Kent State University.

[3] Dey, P. K. (2010), Managing project risk using combined analytic hierarchy process and risk map, in: Applied Soft Computing, Volume 10, 2010, page 1. Retrieved on 12.05.2022 from https://doi.org/10.1016/j.asoc.2010.03.010.

[4] European Commission (2018), "Ethics and data protection. Retrieved on 10.02.2022 from https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

[5] European Commission (2018), "Horizon 2020 Programme Guideance - How to complete your ethics self - assessment". Retrieved on 10.02.2022 from https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[6] European Commission (2018), Ethics in Social Science and Humanities, October 2018.

[7] Farkas, L (2017), Data collection in the field of ethnicity. Analysis and comparative review of equality data collection practices in the European Union, Directorate-General for Justice and Consumer, European Commission, 2017.

[8] GDPR.EU. Retrieved on 10.02.2022 from https://gdpr.eu/what-is-gdpr/.

[9] Grant Agreement Annex 1 part A.

[10] Knottnerus, J. A., Tugwell, P (2018), Ethics of research methodology requires a methodology of research ethics, in: Journal of Clinical Epidemiology, Volume 100, PV-VI, August 01, 2018. Retrieved on 12.05.2022 from https://doi.org/10.1016/J.JCLINEPI.2018.07.001

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

[12] Tang, X, The Ethics of Data Management. Retrieved on 16.05.2022 from PennState, https://sites.psu.edu/ethicsofdatamanagement/.

[13] United Nations Humans Rights, Office of the High Commissioner (2018), A Human Rights-based approach to data. Leaving no one behind in the 2030 Agenda for Sustainable Development, 2018.

[14] UN Women (2021), Counted and Visible: Toolkit to better utilize existing data from household surveys to generate disaggregated gender statistics, Retrieved on 16.05.2022 from https://unstats.un.org/unsd/statcom/52nd-session/documents/BG-3l-Executive_Summary_Counted_and_Visible_Toolkit-E.pdf.

[15] Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018 (2016). https://doi.org/10.1038/sdata.2016.18

Annexes

- **Building Block I Framework T2.3**
- **Building Block II Guideline T2.3**
- **Building Block III Factsheet T2.3**

DIVAIRCITY

The power of Diversity & Inclusion for Climate Neutral Cities

Ethics, privacy and security data management requirements

ANNEX - Framework

ANNEX | Building Block I Framework T2.3

	Norms/standards/requirements	Legal Basis	DivAirCity activities	Risk in colours red (high risk), orange (middle risk) or green (low risk)	Owner(s) of the risks	Controls
GDPR: In research settings, data protection imposes obligations on researchers to provide research subjects with detailed information about what will happen to the personal data they collect.						
General consideration: The lack of a specific data protection structure within the DivAirCity project increases the number and dimension of risks related to privacy. Management of data protection, ethical issues and security needs to be ensured by each partner. This diversification of responsibilities without a single point of control represents a risks and makes it particularly important to: a) identify internal privacy control structures within each partner b) increase coordination efforts in the context of collaborative activities and c) designate responsible parties for essential activities representing risk in terms of privacy, ethics and security.						
	Protection area: All EU projects processing personal information about identifiable human research subjects are subject to the GDPR.	**Art. 1 (1) GDPR:** This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data **Art. 4 (1) GDPR:** 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physicological, genetic, mental, economic, cultural or social identity of that natural person.	As soon as personal data is processed within the meaning of the GDPR, the provision of the GDPR must be observed.		The data controllers are the owner of the risk.	Identification of the data sources and examination of whether personal data is processed within the meaning of the GDPR. If personal data is processed a development of data monitoring process is needed.
	Special categories of personal data: Particular attention should be paid to research involving special categories of data. 'Special categories of personal data' are subject to more stringent data-protection safeguards. They include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.	Art. 9 GDPR: (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (2) Paragraph 1 shall not apply if one of the following applies: a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.	DivAirCity project aims at shifting the urban paradigm by valuing human diversity with a focus on gender and multiculturalism as a resource to define new urban services and models towards cultural-driven green cities. One goal of the project is to create a common, culture-driven framework for co-creation and engagement in cities that takes age, gender, ethnicity, social class, sexual orientation, disabilities and intersectional diversity into account *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 3 and 22)*. Therefore there is a high probability that 'special categories of personal data' within the meaning of Art. 9 GDPR will be processed.		The data controllers (such as the DivAirCity cities) are the owners of the risk.	Identification of what kind of personal data will be processed. If special categories of personal data will be used, obtain a free and fully informed consent of the research participants.
	Profiling: In case the research involves profiling, the beneficiary must provide explanation on how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded. *(Grant Agreement Annex 1 part A, page 53)*	**Art. 4 (4) GDPR:** 'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. **Art. 22 GDPR: (1)** The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. **(2)** Paragraph 1 shall not apply if the decision: **a)** is necessary for entering into, or performance of, a contract between the data subject and a data controller; **b)** is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or **c)** is based on the data subject's explicit consent. (3) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. (4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) or Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.	It must be clarified whether the research involves profiling		The data controllers (such as the DivAirCity cities) are the owner of the risk.	Identification how data will be processed within the DivAirCity project. Profiling should be avoided where possible. In case, profiling is performed, specific processes need to be in place in order to guarantee compliance with GDPR.
	Enlightenment / informed consent: Obligation on researchers to provide research subjects with detailed information about what will happen to the personal data that they collect. This requires consent to be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the subjects's agreement to the processing of their personal data. As a minimum, this should include: the identity of the data controller, the specific purpose of the processing, information as to whether data will be shared with or transferred to third parties and for what purpose, how long the data will be retained before they are destroyed. The data subject must also be made aware if data are to be used for any other purposes, shared with research partners or transferred to organisations outside the EU.	**Art. 4 (11) GDPR:** 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her **Art. 7 GDPR: (1)** Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. **(2)** If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. **(3)** The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. (4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. The data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. (4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. Art. 13 GDPR: (1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: a) the identity and the contact details of the controller and, where applicable, of the controller's representative; b) the contact details of the data protection officer, where applicable; c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party e) the recipients or categories of recipients of the personal data, if any; f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	**It is planned to involve >1500 citizens in the overall co-creation activities** *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part B - Page 9)* . If the personal data of the participants are used then their consent is required. With that many participants there is a high risk of missing informed consent.		The data controllers (such as the DivAirCity cities) are the owners of the risk.	Detailed information on the informed consent procedures in regard to data processing must be kept on file. Templates of the informed consent forms and information sheets (in language and terms intelligible to the participants) must be kept on file. *(Grant Agreement Annex 1 part A, page 53)*

	Purpose limitation, Data minimisation and storage limitation: A data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as it is necessary to fulfil that purpose.	**Art. 5 (1) GDPR:** Personal data shall be: **b)** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation'); **c)** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); **e)** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')	The whole project is obtaining and working with a significant amount of data. On the one hand, there is a risk that data will be stored for an unnecessarily long time. One the other hand there is the risk, that data that is not relevant for the project will be saved.		Each partner within DivAirCity, especially the cities.	Conduct a data minimisation review and a data monitoring process. / The beneficiary must explain how all of the data intended to process is relevant and limited to the purpose of the research project. This must be submitted as a deliverable. *(Grant Agreement Annex 1 part A, page 53)*
	Anonymysation/pseudonymisation of personal data: Anonymise personal data so that it no longer relates to identifiable persons. Data that no longer relates to identifiable persons, such as statistical data, are not personal data and are therefore outside the scope of data protection law.	**Art. 89 (1) GDPR:** Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	Because of the large amount of data, there is a risk that personal data is not anonymised enough.		The data controllers (such as the DivAirCity cities) are the owner of the risk.	Description of the anonymisation / pseudonymisation techniques that will be implemented must be submitted as a deliverable. *(Grant Agreement Annex 1 part A, page 53)*
	Processing of previously collected personal data (secondary use): In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects must be submitted as a deliverable *(Grant Agreement Annex 1 part A, page 53).*	**Art. 13 GDPR: (3)** Where the controller intends to **further process** the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. **(4)** Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	It is necessary to be clarified if the research involves further processing of previously collected data		The data controllers (such as the DivAirCity cities) are the owner of the risk.	Identification what kind of data will be processed within the DivAirCity project.
	Right to be forgotten: In some situations the GDPR gives individuals the right to ask the data controller to delete their personal data.	Art. 17 GDPR: (1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d) the personal data have been unlawfully processed; e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). (2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. (3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: a) for exercising the right of freedom of expression and information; b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or e) for the establishment, exercise or defence of legal claims.	It must be kept in mind, that citizens who's data will be collected may have the right, that their data will be delete, if the relevant legal requirements are met.		The data controllers are the owner of the risk.	Conduct a data processing review so that it can be proven, that data processing and the storage of the data is lawful.
	Data protection / Privacy by design: When planning a processing system, technical and organisational measures must be taken to ensure data security. Consequently the term 'privacy by design' means data protection trough technology design. Data protection can best be observed in data processing operations if it is already technically integrated during their development.	**Art. 25 GDPR: (1)** Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. **(2)** The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. (3) An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.	All processing systems within the DivAirCity project (e.g. Blockchain technology) must take appropriate technical and organisational measures as soon as possible.		The data controllers, who are also operators of processing systems are the owners of the risk.	Conduct a review about the technical and organisational measure which where taken by those responsible.

	Data security: Protect personal data against loss or misuse. The GDPR requires all data controllers and processors to implement appropriate technical and organisational measures to ensure a level of data security that is commensurate to the risks faced by the data subjects in the event of unauthorised access to, or disclosure, accidental deletion or destruction of their data	**Art.32 GDPR: (1)** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: **a)** the pseudonymisation and encryption of personal data; **b)** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; **c)** the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; **d)** a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. **(2)** In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. **(3)** Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. (4) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	The GDPR determines, that depending on the type, scope and purpose of the processing of personal data as well as the different probabilities of occurrence and severity of the risk for the rights and freedoms of natural persons, suitable technical measures must be taken. In this context, particular attention must be paid to the scope and complexity of the data processing, such as the systematic monitoring of a publicly accessible area on a large scale. Furthermore, attention must be paid to data collection or processing techniques such as methods or technologies invading privacy, data mining, including data collected in social networks.		The data controllers and processors are the owners of the risk.	Conduct a review about the technical and organisational measure which were taken by the data controllers and processors.
	Designation of a data protection officer	**Art. 37 GDPR: (1)** The controller and the processor shall designate a data protection officer in any case where: **a)** the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; **b)** 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 **c)** 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 or personal data relating to criminal convictions and offences referred to in Article 10. **(2)** A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. **(3)** Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size. **(4)** In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors. (5) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. (6) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. (7) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	It must be clarified whether and where a data protection officer ist required. For cities, which are a public authority or body, there must be a data protection officer appointed (according to Art. 37 (1) a)).		Data controllers and processors.	
	Use of Blockchain Technology	DivAirCity will enable cities to create decentralised business models where people interact with each other according to a protocol specified in code and enforced on the blockchain. This will enable not only more social inclusion but also equip public authorities to be less dependent on central government in terms of funding and budgets (Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part B - Page 20).	DivAirCity will deliver a solution to introduce citizens participation and reward for their contribution to Air Quality in each of the cities. Each city will develop its own rewarding method and tokenisation model.		Cities.	Each city will control prior to implementation of any blockchain based solution that compliance wit GDPR is ensured. Personal data even if it is hashed may not be directly introduced into any blockchain. Data protection responsible must provide a privacy, ethical and security risk analisys of the provided platform.
Ethics: All projects are guided by ethical considerations and the values and principles on which the EU is founded						
	Involvement of Human Participants *(Grant Agreement Annex 1 part B, page 141)* : A research involves human participants if you recruit them directly or if the research activities consist of actively involving, influencing, manipulating or directing people in any way.	If you work with Human Participants, particular attention must be paid to the following groups of people (based on the ethics issues checklist of Horizon 2020 Programme, Guidance, How to complete your ethics self-assessment, pages 6-11): - Volunteers for social or human science research - Persons who are unable to give informed consent - Children and minors - Vulnerable individuals or groups - People with disease / medial condition / disability	Citizens/people (human participants), and their diversity, are key resources of the DivAirCity project in tackling air pollution and climate challenges. *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part B - Page 8)* . There is a risk that people and human dignity will not be respected and that a fair distribution of the benefits and burden of research cannot be ensured.		Data controllers	Provide a detailed analysis of the ethical issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that - are written in a language and in terms they can fully understand - describe the aims, methods and implications of the research - explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time without any consequences.
	Involvement of physical interventions on the study participants *(Grant Agreement Annex 1 part B, page 141)* : A research involves physical intervention on the study participants if there are invasive techniques involved such as collection of human cells or tissues or medical interventions		There will be a health impact evaluation. Health will be assessed by measuring vital signs using wearables, e.g. heart rate, blood oxygen saturation, temperature, and electrodermal activity *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 40)* . There is a risk that people and human dignity will not be respected and that a fair distribution of the benefits and burden of research can not be ensured.		Data controllers	Provide a detailed analysis of the ethical issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that: - are written in a language and in terms they can fully understand - describe the aims, methods and implications of the research - explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time without any consequences.
	Other ethics issues *(Grant Agreement Annex 1 part B, page 142)* : Is it ethical to incentivise human beings to act in a certain way?		Financial incentives are created. In addition, an incentive system that goes beyond the mechanisms of financial incentives is integrated into the entire public participation process. Examples are: certificate launched by the Municipalities to recognise the participation and associate the participation with a waste tax reduction of 10% during the duration of the project. Creation of a job Bank for the project activities and those people who participate in the co-creation activities will be given extra points. These kind of incentives could be viewed as a form of undue influence *(Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 22).* It is also questionable whether the anticipated incentives evoke behaviours that would not take place without the incentive. Besides all the basic census data will follow biological categorisation of human beings such as gender and ethnicities, and inevitably, other collected data will also be cross-referenced with this biological categorisation. Is it ethical to represent them through this fixed categorisation? How can we show the participants as partners of co-creation, not as 'victims' of systems or inequality? In the context of the DivAirCity project it is necessary to conduct a certain breakdown of data, but stigmatsation should be avoided.		Data controllers	Every co-creation activity as well as the design of incentives must be accompanied by a report that analises possible ethical risks of the activities and shall only be performed in case an informed evaluation ensures respect of ethical principles.

DIVAIRCITY

The power of Diversity & Inclusion for Climate Neutral Cities

Ethics, privacy and security data management requirements

ANNEX – Guideline

Table of Contents

A) Objectives of this Guideline (T2.3.)

Before the objectives of this Guideline are described, some **introductory words** shall be outlined in order to understand the why this document exists.

According to the Grant Agreement, "DivAirCity will create a set of real action tools and interventions, linked to challenges and objectives, to migrate, adapt and monitor air pollution and carbon challenges in five selected EU cities trough: […] An equal representation of data"[1].

The consortium has stated in the proposal, that "the existing bias in data is often an unspoken territory. Data sets, data frameworks, Big Data in the modern world are the hidden places where inequality still resides. […] Data not only describes the world, but it is used to shape it. This is the reason why the approach to Data Management in DivAirCity is the first initial step to shape inclusive solutions to mitigate air pollution and climate issues in cities"[2].

Therefore, the primary objective of WP2 is to provide the data analytics framework for the entire DivAirCity project, which will enable decision making and management of social involvement, through a strong Diversity and Inclusion Data Framework[3].

Within WP2, Task 2.3 focuses on "identification of ethics, privacy and security data management requirements. This task will deliver the **Framework**, **Guideline** and **Operational tools** for the implementation of the GDPR, legal and ethics related data management requirements at a national and EU level"[4]. We suggest that all DivAirCity partners implement the Framework, Guideline and Operational tools in all deliverables after April 2022.

This Guideline incorporates the GDPR and ethics related personal data management risks that have been mentioned by DivAirCity partners as such and shall be an easy-to-read instruction and support document for all DivAirCity partners and especially for the cities within the project. The Guideline does not consider *The Proposal for a Regulation of the European Parliament and the Council on harmonized rules on fair access to and use of data (Data Act)*. The aim of the *Data Act* is to ensure fairness in the allocation of value from data

[1] Grant Agreement Annex 1 part B, page 9.
[2] Grant Agreement Annex 1 part B, pages 20, 21.
[3] Grant Agreement Annex 1 part A, page 18 of 61.
[4] Grant Agreement Annex 1 part A, page 19.

among actors in the data economy and to foster access and use of data[5]. Thus, the *Data Act* is complementing existing rights, specifically those regarding data generated by a users' product connected to a publicly available electronic communications network[6]. Therefore, the *Data Act* is not relevant for the objective of Task 2.3, which is the protection of personal data from citizens according to the GDPR.

[5] Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), 2022, page 2, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN (last access on 30.03.2022).

[6] Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), 2022, page 3,4, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN (last access on 30.03.2022).

B) Method and methodology

Our overall approach for this Guideline is the participatory methodology[7]. This leads to taking into account the social atmosphere and taking input from the DivAirCity partners, especially the cities, when developing the GDPR requirements and ethics issues.

In relation with the objective of Task 2.3, there are several overlaps with other WPs, such as WP1 and WP9 regarding the Data management Plan and DM officer appointment (D1.6), Ethical Board Member List (D1.9), Legal and IPR requirements report (D.11), Requirement No. 2 (D9.1) and Requirement No. 3 (D9.2). Therefore, a set of activities have been performed to ensure cooperation with the two referred WPs. The Ethical Charter (D1.7) focuses on the internal DivAirCity structure and serves as Code of Conduct for and within the Consortium and its member organizations. It does not involve the ethical research aspects and or data management issues and for this reason we don't refer to the Ethical Charter in the Guideline.

In addition, desk research such as literature review and legal text interpretation method of GDPR and other legal related data management requirements at EU level have been performed:

- European Commission (2018), Ethics and data protection, 14 November 2018.
- European Commission (2018), Ethics in Social Science and Humanities, October 2018.
- European Agency for Cybersecurity (ENISA), Deploying Pseudonymisation Techniques, 2022.
- Horizon 2020 Framework Programme of the European Union, GDPR. eu, https://gdpr.eu/
- Information Commissioner's Office, Determining what is personal data, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

[7] Thiollent, M (2011), Action Research and Participatory Research: An Overview, in International Journal of Action Research, 7 (2011) 2, page 1, in https://nbn-resolving.org/urn:nbn:de:0168-ssoar-414079 (last access on 16.05.2022).

- United Nations Development Programme (UNDP), Data Futures Platform, 8 Data Principles for UNDP, https://data.undp.org/data-principles/
- United Nations Development Group (2017), Data Privacy, Ethics and Protection, Guidance note on big data for achievement of the 2030 Agenda.

For national level, partners will have to refer to their Data Protection Officers or similar.

A literature review has been performed and focus has been given to the following documents:

- ALLEA, The European Code of Conduct of Research Integrity, 2017.
- European Commission (2019), Horizon 2020 Programme, Guidance. How to complete your ethics self-assessment, 4. February 2019.
- Farkas, L (2017), Data collection in the field of ethnicity. Analysis and comparative review of equality data collection practices int eh European Union, Directorate-General for Justice and Consumer, European Commission, 2017.
- United Nations Humans Rights, Office of the High Commissioner (2018), A Human Rights-based approach to data. Leaving no one behind in the 2030 Agenda for Sustainable Development, 2018.
- Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018 (2016). https://doi.org/10.1038/sdata.2016.18

Text interpretation method and analysis of the activities planned within DivAirCity leads to the ethics requirements (see D9.2) and ethics issues.

In order to link the ethics related data management requirements with the DivAirCity related activities, especially the activities of the five cities and WP5 D&I SCCC, partners have been asked to fill in their planned activities under point D) below.

Interviews with the relevant DivAirCity partners such as the cities have taken place focusing on the identification of their activities that imply recompilation of personal data from citizens.

C) GDPR and ethical requirements for data management within the DivAirCity project

I. What has GDPR to do with DivAirCity?

The General Data Protection Regulation (GDRP) is a privacy and security regulation which is directly applicable throughout the EU. Apart from GDPR, all EU Member States have their own national data protection legislation which may be even stricter than GDPR. Partners need to make sure they are fully compliant with all EU and national applicable legislation. Therefore, please do check with your local data protection officer (DPO) or data protection responsible that you comply with your **national** data protection legislation.

Though the GDPR, which was drafted and passed by the EU, it imposes obligations onto organizations anywhere, as long as they target or collect **personal data** related to **citizens in the EU**. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching tens of millions of euros[8].

In general, **personal data** is any information that allows a living natural person to be directly, or indirectly, identified from data that is available. This might be a **person's name**, **location data**, or a **clear online username** but it also may be less immediately apparent information such as **IP addresses, cookie identifiers or several characteristics, which express the physical, physiological, genetic, mental, commercial, cultural or social identity of the natural person.**

In practice, it also includes all data which are or can be assigned to a person in any kind of way (telephone, credit card, personnel number of a person, account data, number plate...etc.). The term personal data should be interpreted as broadly as possible. For instance, notes taken by a facilitator in a cocreation activity would be deemed personal data if the person can be theoretically identified.

The crucial thing about what constitutes personal data is that it allows a person to be identified. In this sense, **pseudonymised data** can still fall under the definition of personal data in case a person can be identified from it.

[8] GDPR.EU: https://gdpr.eu/what-is-gdpr/ (last access on 01.02.2022).

A few special categories of **sensitive personal data** are given greater protections: racial or ethnic origin, political opinions, religious beliefs, membership of trade unions, genetic and biometric data, and data around a person's sex life or orientation. As a general rule, it is prohibited to process this kind of data. However, if you have received explicit consent to the processing of that personal data for specified purposes like the case of DivAirCity if processing is necessary for scientific research purposes (Art. 9.2 j GDPR).

'**Controllers**' are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. It is also possible that there are joint controllers of personal data, where two or more groups determine how data is handled. It can be assumed that especially the cities in the project are controllers of personal data (of citizens).

'**Processors**' act on behalf and only on the instructions of the relevant controller. Controllers have stricter obligations under GDPR than processors. It can be assumed that many other partners within the project, that are not cities, act/will act as processors of the project.

An independent Ethics Screening by independent Ethics experts contracted by European Commission have already identified GDPR issues that are relevant for DivAirCity. They have become part of the Grant Agreement by integrating them in Workpackage (WP) 9 as the so-called Ethics Requirements No. 3. Although they are GDPR related issues, European Commission treats them as Ethics issues or Ethics Requirements.

As per Ethics Requirement No. 3, DivAirCity is obliged to focus on the following data protection issues, which were developed by the Ethics Panel of the European Commission and not by T.2.3:

- The beneficiary must explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation' principle).
- Description of the anonymisation/pseudonymisation techniques.
- Detailed information on the informed consent procedures regarding data processing.
- Templates of the informed consent forms and information sheets (in language and terms intelligible to the participants).
- In case the research involves profiling, the beneficiary must provide explanation on how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded.

- In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organizational measures are in place to safeguard the rights of the data subjects is required.

II. Ethic related data management requirements

Furthermore, there are ethics related data management requirements that the project must comply with. These have also been identified by the same Ethics Screening as mentioned above and have become part of the Grant Agreement by incorporating them in WP9, being included as Ethics Requirements No.2[9]. These requirements will be listed here below and they will be tackled by WP9.

These requirements are:

- The procedures and criteria that will be used to identify/recruit research participants must be submitted as a deliverable.
- The informed consent procedures that will be implemented for the participation of citizens must be submitted as a deliverable.
- Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) must be kept on file.
- Copies of opinions/approvals by ethics committees and/or competent authorities for the research with citizens must be kept on file.

[9] Grant Agreement Annex 1 part A, page 53.

D) Implementation of GDPR and Ethics related data management requirements

In the following, you can find a summary of the GDPR and ethics related issues that have been identified as potential data that you, as a DivAirCity partner, who works with citizens personal data, may deal with. The purpose of this document is to raise your awareness as to the importance to be compliant when dealing with personal data and to provide you with orientation as to how to react and mitigate the risk. The spirit of DivAirCity is to foster the exchange of information with citizens and this Guideline attempts to assist you in understanding the importance and interpretating the key relevant issues.

First of all, it must be checked whether the processed data falls within the protection area of the GDPR (I.1.). If this is the case, as a next step special attention must be paid if 'special categories of data' (I.2.) are processed and if during the processing 'profiling'(I.3.) is used. As soon as these aspects have been clarified, you should ensure that the principles of data processing are observed (I.4., I.5., I.6.). Further important aspects of the GDPR are the secondary use of Data (I.7.) as well as the 'right to be forgotten'(I.8.). Finally, the foreseen technical-organizational measures (I.9., I.10., I.11.) must be implemented.

It is important that you are aware of any specific national legislation regarding privacy, data protection, ethical issues and security.

You need to ensure that the necessary measures are in place in order to be fully compliant with any legislation applicable in your jurisdiction.

I. GDPR

1. Protection Area of the GDPR

As you already know, the GDPR regulates the processing of personal data.

Therefore, all EU projects processing personal information about identifiable human research subjects are subject to the GDPR. That means, that you, as a DivAirCity partner, are obliged to comply with the GDPR as well as any other legislation applicable at national or local level.

According to the GDPR '**personal data**' means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person for example.

a) DivAirCity activities / risks

As soon as personal data is processed within the meaning of the GDPR, the provision of the GDPR must be observed.

b) Owner of the risk

The data controllers[10] are the owner of the risk.

c) Controls

Identification of the data sources and examination of whether personal data is processed within the meaning of the GDPR. If personal data is processed a development of data monitoring process is needed.

[10] ” Controller" in the sense of Art. 4 (7) GDPR means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

2. Special categories of personal data

As a partner of DivAirCity you should pay particular attention to research involving **'special categories of data'**. They can be subject to more stringent data-protection safeguards.

Special categories of data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. At least one condition listed must be fulfilled to process special categories of data. You are for example processing biometric data as a form of 'special categories of data', when you are collecting data with facial recognition, fingerprints, voice recognition or palmprint verification.

a) DivAirCity activities / risks

DivAirCity project aims at shifting the urban paradigm by valuing human diversity with a focus on gender and multiculturalism as a resource to define new urban services and models towards cultural-driven green cities. One goal of the project is to create a common, culture-driven framework for co-creation and engagement in cities that takes age, gender, ethnicity, social class, sexual orientation, disabilities and intersectional diversity into account[11]. Therefore, there is a high possibility that 'special categories of personal data' within the meaning of Art. 9 GDPR will be processed.

b) Owner of the risk

The data controllers are the owners of the risk.

c) Controls

Identification what kind of personal data will be processed. If special categories of personal data will be used, obtain a free and fully informed consent of the research participants (Art. 9(2) GDPR) and follow all the relevant provisions related thereto.

[11] Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 3 and 22.

3. Profiling

It is also important for you as a partner of DivAirCity to check whether your research includes the process of 'profiling'.

Profiling in the context of the GDPR means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

Profiling can be used to analyse the natural person's performance at work, economic situation, health, interests, behavior, location or movements for example.

In case your research involves profiling, the data subject needs to be informed of the existence of profiling and the associated consequences. This is why you must provide an explanation on how the data subjects will be informed of the existence of the profiling, its possible consequences and how their fundamental rights will be safeguarded[12].

a) **DivAirCity activities / risks**

It must be clarified whether the research involves profiling.

b) **Owner of the risk**

The data controllers are the owner of the risk.

c) **Controls**

Identification how data will be processed within the DivAirCity project.

[12] Art. 22 (2) GDPR, also Grant Agreement Annex 1 part A, page 53, Ethic Requirements No. 3.

4. Enlightenment / informed consent

People have a right to know what data an organization collects, why it collect it and what it does with it. Therefore, there is an obligation on researchers to provide subjects with detailed information about what will happen to the personal data that they collect. This requires the consent of those affected. This consent must be given through a clear and voluntary act.

In addition, the GDPR also prescribes that the individual whose data is being collected must provide some information. This information includes the identity of the data controller, the specific purpose of the processing, information as to whether data will be shared with or transferred to third parties and for what purpose, how long the data will be retained before it is destroyed.

a) DivAirCity activities / risks

It is planned to involve >1500 citizens in the overall co-creation activities[13]. If the personal data of the participants are used, then their consent is required. With such a high number of participants there is a high risk of missing/lacking informed consents.

b) Owner of the risk

The data controllers are the owners of the risk.

c) Controls

Detailed information on the informed consent procedures in regard to data processing must be kept on file. Templates of the informed consent forms and information sheets (in language and terms intelligible to the participants) must be kept on file[14].

[13] Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part B - Page 9.
[14] Grant Agreement Annex 1 part A, page 53.

5. Purpose limitation, data minimization and storage limitation

When processing data, one should keep in mind, that it must be done in a lawful, fair and transparent manner.

That is why a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a **specified purpose** (the so-called '**data minimisation**' principle). That means that within DivAirCity not all personal data can be collected and then later the decision will be taken, which data is useful for the project. On the contrary, first, the relevant partner has to decide which personal data is necessary (on the basis of appropriate justification) and then, this data will be collected if it is deemed necessary and only to the extent it is.

In addition, it should be noted that personal data shall only be collected for specified, explicit and legitimate purposes ('**purpose limitation**' principle). In this case, only personal data related to DivAirCity activities can be collected.

Furthermore, a data controller should also retain the data only for as long as is necessary to fulfil that purpose ('**storage limitation**' principle).

a) DivAirCity activities / risks

The whole project is obtaining and working with a significant amount of data. On the one hand, there is a risk that data will be stored for an unnecessarily long time. One the other hand, there is the risk that data that is not relevant for the project will be collected and stored.

b) Owner of the risk

The data controllers are the owner of the risk.

c) Controls

Conduct a data minimisation review and a data monitoring process. / The beneficiary must explain how all of the data it intends to process is relevant and limited to the purpose of the research project. This must be submitted as a deliverable[15].

[15] Grant Agreement Annex 1 part A, page 53.

6. Anonymisation / pseudonymisation of personal data

You as a partner should keep in mind, that the principles of the GDPR do not apply to anonymous information. Anonymous information does not relate to an identified or identifiable natural person or to personal data.

The European Commission offers this distinction[16]:

"Pseudonymisation and anonymisation are not the same thing and it is important that you are aware of the difference between them, as the GDPR requires you to use them wherever possible or feasible."

"***Pseudonymisation*** *entails substituting personally identifiable information (such as an individual's name) with a unique identifier that is not connected to their real-world identity, using techniques such as coding or hashing. However, if it is possible to re-identify the individual data subjects by reversing the pseudonymisation process, data protection obligations still apply. They cease to apply only when the data are fully and irreversibly anonymised.*

Anonymisation *involves techniques that can be used to convert personal data into anonymised data. Anonymisation is increasingly challenging because of the potential for re-identification.*

Re-identification *is the process of turning pseudonymised or anonymised data back into personal data by means of data matching or similar techniques."*

"While anonymised data is no longer considered personal data, anonymisation processes are challenging, particularly where large datasets containing a wide range of personal data are concerned. This is because it is very difficult to create fully anonymous datasets that retain the granular information needed for research purposes. As far as your research proposal is concerned, if there is a significant prospect of re-identification of persons whose data have been collected, the information should be treated as personal data. (…) If you intend to anonymise the data you collect for use in your research project, the timing of the anonymisation process is paramount. You are collecting 'anonymised' data only if the anonymisation happens at the point and time at which the data are collected from the research subject, so that no personal data are actually processed. If anonymisation takes place at a later stage, e.g., you intend to remove personally identifiable information during the transcription of audio recordings or at the point at which survey data are fed into a database, the raw data are still personal data and your proposal must include provisions for their protection up until the point at which they are deleted or rendered anonymous.

In some instances, your host institution, funding body or publisher may require you to keep the raw data for auditing, accountability or research integrity purposes. There

[16] Ethics and Data Protection, 5 July 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf (last access on 01.02.2022), page 8-9.

may be other scenarios in which a host institution has a raw dataset which it makes available to its researchers and partners in anonymised form. In these instances, while the recipients of the anonymised data may – subject to the mitigation of the risk of re-identification – be exempt from data protection requirements, the host institution is still processing personal data and must therefore ensure appropriate protection for the raw (personal) data. This includes technical and organizational measures to protect the data and the means to identify the data subjects (e.g., the keys, codes or applications used to anonymise the data) against unauthorized access or use. If you are in any doubt as to the adequacy of the technique(s) that you intend to use, you should seek advice from your DPO or a suitably qualified expert. As noted below (see Box 5), for sensitive or complex processing scenarios involving pseudonymisation or anonymisation, it may even be necessary to conduct a DPIA in order to ensure an appropriate level of data protection and minimize risk to the data subjects' rights."[17]

In order to make things easier within the project it can therefore be useful to anonymise personal data so that they no longer relate to identifiable individuals. Data that no longer relate to identifiable persons, such as statistical data, are not personal data and are for this reason outside the scope of data protection law. Ethics Requirements No. 3 Point 4.8. states in this context, that the description of the anonymisation/pseudonymisation techniques that will be implemented must be submitted as a deliverable. For further information about pseudonymisation techniques, it is suggested to consider the document publication *Deploying Pseudonymisation Techniques* issued by the European Agency for Cybersecurity (ENISA)[18].

a) DivAirCity activities / risks

Because of the large amount of data, there could be a risk that personal data is not anonymised. In particular, it is identified that the citizens rewarding system to be developed under WP5 might need the processing of not anonymised nor pseudoanonimised personal data. The specific focus on diversity groups for which personal information might be particularly sensitive (race, religion, nationality, social status, etc.), increases the risk related to pseudoanonimisation and the potential (even if only remotely) identification of pseudoanonimised data.

b) Owner of the risk

The data controllers are the owner of the risk.

c) Controls

[17] Ethics and Data Protection, 5 July 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf (last access on 01.02.2022), page 9.
[18] Enisa, Deploying Pseudonymization Techniques https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques (last access on 30.03.2022).

Description of the anonymisation / pseudonymisation techniques that will be implemented must be submitted and subject to control as a deliverable[19].

7. Processing of previously collected personal data (secondary use)

Caution is also required when processing personal data that has already been collected in advance (by other researchers or in social media, etc.). In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects must be submitted as a deliverable[20].

a) DivAirCity activities / risks

It is necessary to clarify if the research involves further processing of previously collected data.

b) Owner of the risk

The data controllers are the owner of the risk.

c) Controls

Identification of what kind of data will be processed within the DivAirCity project. Confirmation of the beneficiary's lawful basis for the treatment of the information and set up of the appropriate controls.

[19] Grant Agreement Annex 1 part A, page 53.
[20] Grant Agreement Annex 1 part A, page 53, Ethic Requirements No. 3.

8. The 'Right to be forgotten'

In some situations, the GDPR gives individuals the right to request the data controller to delete their personal data. Otherwise, the right to control one's data would be meaningless if individuals could not subsequently contradict the processing of their data. In cases where people no longer consent to the processing, when the data contains material errors, when the processing itself was unlawful or when they believe information is being held unnecessarily, individuals may request that their data be erased[21]. Since the GDPR does not specify what a valid erasure request must contain, the deletion can be requested verbally or written form.

a) DivAirCity activities / risks

It must be kept in mind, that citizens whose data will be collected have the right to submit a deletion request and that their data then must be deleted, if the relevant legal requirements are met.

b) Owner of the risk

The data controllers are the owner of the risk.

a) Controls

Conduct a data processing review so that it can be proven, that data processing and the storage of the data is lawful. Mechanisms to exercise the right to be forgotten must be in place and easy to identify by any individual in order to facilitate their access.

[21] GDPR.eu, https://gdpr.eu/right-to-be-forgotten/ (last access on 02.03.2022).

9. Data protection / privacy by design

When planning a data processing system, technical and organisational measures must be taken as early as possible to ensure that data security is guaranteed and that data protection principles are observed. Consequently, the term 'privacy by design 'means that data protection is considered in every step of the project, starting by the design and planning of the activities and to the ultimate implementation. Processes and available technological means shall be applied for the purpose of a privacy sound project. Any activities planned and discussed should be considered from the perspective of personal data protection applicable rules and regulations. For instance, measures in this sense consist of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to functions and processing of personal data[22].

a) DivAirCity actives / risks

All processing systems within the DivAirCity project (e.g., Blockchain technology) must take appropriate technical and organizational measures as soon as possible.

b) Owner of the risk

The data controllers, who are also operators of processing systems, are the owners of the risk.

c) Controls

Every planned activity must include a data privacy risk analysis and control. Review all technical and organizational measures to be taken by the responsible person, before an activity or initiative or similar takes place.

[22] Regulation (EU) 2016/679 of the European Parliament and to the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE, (last access on 03.03.2022), page 15.

10. Data security

Since the GDPR aims to protect data against loss or misuse, you as a partner should also keep this in mind. The GDPR requires all data controllers and processors to implement appropriate technical and organisational measures in this respect.

Technical measures mean anything from requiring your team to use two-factor authentication on accounts where personal data is stored to contracting with cloud providers that use end-to-end encryption[23].

Organisational measures are things like staff trainings, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it[24]. This is intended to ensure an appropriate level of data security.

a) DivAirCity activities / risks

The GDPR determines, that depending on the type, scope and purpose of the processing of personal data as well as the different probabilities of occurrence and severity of the risk for the rights and freedoms of natural persons, suitable technical measures must be taken. In this context, particular attention must be paid to the scope and complexity of the data processing, such as the systematic monitoring of a publicly accessible area on a large scale. Furthermore, attention must be paid to data collection or processing techniques such as methods or technologies invading privacy, data mining, including data collected in social networks.

d) Owner of the risk

The data controllers and processors are the owners of the risk.

b) Controls

Conduct a review about the technical and organisational measure which were taken by the data controllers and processors.

[23] GDPR.eu, https://gdpr.eu/what-is-gdpr/ (last access on 01.02.2022).
[24] GDPR.eu, https://gdpr.eu/what-is-gdpr/ (last access on 01.02.2022).

11. Designation of a data protection officer

Under certain circumstances the GDPR requires the controller and the processor to designate a data protection officer. What is a data protection officer (DPO)? In your case the DPO is the contact point within the project for questions regarding the GDPR. This individual has expert knowledge of privacy laws and privacy practices. The respective state law regulates whether a data protection officer is necessary. If a DPO is no required in your country, it still is advisable to appoint a responsible for the GDPR in order to keep track of this area.

a) DivAirCity activities / risks

It must be clarified whether and where a data protection officer is required. For cities, this is always the case since each city needs to appoint a DPO.

b) Owner of the risk

Data controllers and processors.

c) Controls

DPO's need to be designated as appropriate and work in full control of the activities of DivAirCity in order to contribute to a 'Privacy by Design' project development and execution.

II. Ethics

12. Involvement of Human Participants[25]

Research involves human participants if you recruit them directly or if the research activities consist of actively involving, influencing, manipulating or directing people in any way.

If you work with Human Participants particular attention must be paid to the following groups of people:

- Volunteers for social or human science research
- People who are unable to give informed consent. That includes those who are not able to make decision due to their free will, for instance mentally ill people or people with intellectual disabilities.
- Children and minors
- Vulnerable individuals or groups
- People with disease / medical condition / disability

a) DivAirCity activities / risks

Citizens/people (human participants), and their diverse mix, are key resources of the DivAirCity project in tackling air pollution and climate challenges[26]. There is a risk that people and human dignity will not be respected and that a fair distribution of the benefits and burden of research cannot be ensured.

b) Owner of the risk

Data controllers

c) Controls

Provide a detailed analysis of the ethics issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that:

- Are written in a language and in terms they can fully understand
- Describe the aims, methods and implications of the research
- Explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time without any consequences
- Therefore, it could be necessary to include ethics and security training for facilitators in cities

[25] Grant Agreement Annex 1 part B, page 141.
[26] Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part B - Page 8.

13. Involvement of physical interventions on the study participants[27]

Research involves physical intervention on the study participants if there are invasive techniques involved such as collection of human cells or tissues or medical interventions

a) DivAirCity activities / risks

There will be a health impact evaluation. Health will be assessed by measuring vital signs using wearables, e.g., heart rate, blood oxygen saturation, temperature, and electrodermal activity[28]. There is a risk that people and human dignity will not be respected if a fair distribution of the benefits and burden of research cannot be ensured.

b) Owner of the risk

Data controllers

c) Controls

Provide a detailed analysis of the ethics issues. Further obtain a free and fully informed consent of the research participants. Participants must be given an informed consent form and detailed information sheets that:

- Are written in a language and in terms they can fully understand.
- Describe the aims, methods and implications of the research.
- Explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time without any consequences.

[27] Grant Agreement Annex 1 part B, page 141.
[28] Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 40.

III. Other ethical issues [29]

14. Ethical consideration regarding potential human manipulation derived from citizens' incentives and rewards

a) DivAirCity activities / risks

Is it ethical to incentivise human beings to act in a certain way?

Financial and other incentives are foreseen within DivAirCity in view of: a) fostering and rewarding participation and b) fostering behaviors that contribute to AQ in the Cities. An example would be the issuance of a certificate by the Municipalities to recognize the participation associated to a waste tax reduction of 10% during the duration of the project. Another example would be the creation of a job Bank for the project activities and those people who participate in the co-creation activities will be given extra points. Public policy is generally based on creating sanctions and incentives to achieve a specific social model under consensus established in national parliaments and other public spheres. However, there is an intrinsic ethical risk in specifically affecting individual´s behavior under a strongly conductive approach. These kinds of incentives could be viewed as a form of undue influence[30]. It is essential to reflect on the potential effects of rewards and incentives both on individuals and in at a social level.

b) Owner of the risk

Data controllers

c) Controls

Use of European Code of Conduct of Research Integrity. Any doubt raised or identified in this respect should be escalated to the DivAirCity Management Team and treated with the upmost carefulness. Furthermore, the Ethical Board members (D1.9) should be involved.

[29] Grant Agreement Annex 1 part B, page 142.
[30] Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 22.

15. Risk of stigmatisation as a consequence of data

a) DivAirCity activities / risks

DivAirCity project aims at shifting the urban paradigm by valuing human diversity with a focus on gender and multiculturalism as a resource to define new urban services and models towards cultural-driven green cities. One goal of the project is to create a common, culture-driven framework for co-creation and engagement in cities that takes age, gender, ethnicity, social class, sexual orientation, disabilities and intersectional diversity into account[31]. All the basic census data will follow biological categorization of human beings such as gender and ethnicities. Inevitably, other collected data will also be cross-referenced with this biological categorization. Is it ethical to represent them through this fixed categorisation? How can we show the participants as partners of co-creation, not as victims of systems or inequality? In the context of the DivAirCity project it is necessary to conduct a certain breakdown of data, but stigmatisation should be avoided.

b) Owner of the risk

Data controllers

c) Controls

Use of European Code of Conduct of Research Integrity.

According to the United Nations Human Rights Office of the High Commissioner, the participation is central to a human rights-based approach[32] 'individuals should have the option to disclose, or withhold, information about their personal characteristics'. Make sure to be very respectful with the data subjects involved in your activities.

Any doubt raised or identified in this respect should be escalated to the DivAirCity Management Team and treated with the upmost carefulness. Furthermore, the Ethical Board members (D1.9) should be involved.

[31] Grant Agreement Number 101003799 - DivAirCity - Annex 1 Part A - Page 3 and 22.
[32] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data, page 11.

16. Risk of non-inclusion

a) DivAirCity activities / risks

One of DivAirCity' s many objectives is to value human diversity. Therefore, partners who interact with research participants should be as inclusive as possible when reaching out to research subjects. According to the United Nations Human Rights Office of the High Commissioner, the participation is central to a human rights-based approach[33]. It is instrumental to the realization of all components of the human rights-based approach 'as well as retaining trust in official and other relevant data and statistics'[34].

b) Owner of the risk

Data controllers

c) Controls

Use of European Code of Conduct of Research Integrity.
Make sure to be as inclusive as possible when designing your activities/events/initiatives. Any doubt raised or identified in this respect should be escalated to the DivAirCity Management Team and treated with the upmost carefulness. Furthermore, the Ethical Board members (D1.9) should be involved.

[33] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data, page 3.
[34] See above.

17. Risk of no data disaggregation

a) DivAirCity activities / risks

DivAirCity intends to obtain special category of data (see above, point 3.2) from research subjects and needs this data in order to be able to 'value human diversity'. Some Member States such as France and Romania prohibit the collection of personal data revealing racial or ethnic origin [35]. The UN Special Rapporteur on Extreme Poverty and Human Rights has suggested that European Commission should start an infringement procedure if a Member State continues to misinterpret the GDPR as not permitting data collection on the basis of racial and ethnic origin[36].

b) Owner of the risk

Data controllers

c) Controls

Use of European Code of Conduct of Research Integrity.
If you encounter any difficulties in being able to collect personal data revealing racial or ethnic origin do reach out to the DivAirCity Management Team and the Ethical Board members (D1.9).

[35] LaBreck, Abby, Color-Blind: Examining France's Approach to Race Policy, in: Harvard International Review, 01.02.2021, available in: https://hir.harvard.edu/color-blind-frances-approach-to-race/ (last access on 11.05.2022).
[36] Farkas, Lilla (2017): Analysis and comparative review of Equality data collection practices in the European Union. Data collection in the field of ethnicity, Report, Directorate-General for Justice and Consumers, 2017, page 5.

18. Risk of no transparency

a) DivAirCity activities / risks

Within the DivAirCity project, some consortium partners will obtain personal data from research subjects and some of these partners are cities and therefore public authorities. According to the United Nations Human Rights Office of the High Commissioner, it is very important that data collectors provide clear, openly accessible information about their operations, including research design and data collection methodology; especially the data collected by public authorities such as the cities should be openly accessible to the public[37]. The same goes for the ALLEA European Code of Conduct for Research Integrity[38] and the FAIR Principles[39] which require 'researchers ensure access to data is as open as possible, as closed as necessary, and where appropriate in line with the FAIR Principles (Findable, Accessible, Interoperable and Re-usable) for data Management' (section 2.5 of the ALLEA European Code of Conduct for Research Integrity).

b) Owner of the risk

Data controllers

c) Controls

Use of European Code of Conduct of Research Integrity.
Make sure to make public how is collected and to disseminate it as quickly as possible after collection. If you encounter any difficulties in being able to be transparent do reach out to the DivAirCity Management Team and the Ethical Board members (D1.9).

[37] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data, page 14.
[38] ALLEA, The European Code of Conduct for Research Integrity, in: https://allea.org/code-of-conduct/, 2017 (last access on 16.05.2022).
[39] Wilkinson, M., Dumontier, M., Aalbersberg, I. *et al.* The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data* **3,** 160018 (2016). https://doi.org/10.1038/sdata.2016.18 2017 (last access on 16.05.2022).

19. Risk of no accountability

a) DivAirCity activities / risks

As mentioned before, some of the DivAirCity research partners are cities and therefore public authorities. According to the United Nations Human Rights Office of the High Commissioner, "data collectors are accountable for upholding human rights in their operations, and data should be used to hold States and other actors to account on human rights issues"[40]. Cities have to be aware of the fact that they are human rights duty-bearers and as such they have "the obligation to respect, protect and fulfil human rights in their daily exercise of statistical activities"[40].

b) Owner of the risk

Data controllers

c) Controls

Use of European Code of Conduct of Research Integrity.
If you encounter any difficulties in being able to uphold human rights in your (data management) operations reach out to the DivAirCity Management Team and the Ethical Board members (D1.9).

[40] United Nations Human Rights Office of the High Commissioner (2018), A human-rights-based approach to data, page 18.

DIVAIRCITY

The power of Diversity & Inclusion for Climate Neutral Cities

Ethics, privacy and security data management requirements

ANNEX - Factsheet

Within the DivAirCity project some activities might generate GDPR and ethic related issues. This Factsheet will give an overview of such activities which might be affected:

Activities regarding the observation of air pollution	
Activities	**GDPR and Ethic Related Issues**
Activities that the DivAirCity partners might undertake regarding the observation of air pollution: - Exchange with citizens about their knowledge and experiences about air pollution at home, at school or work - Measurements of the air pollution at home, at school or work with sensor technology - Measurements of the air pollution on the routes taken by the citizens with sensor technology - Public space observation	If DivAirCity partners are planning such activities, the following must be considered: With these activities DivAirCity partners are collecting personal data in the meaning of the GDPR. Therefore, a consent of those affected is required *(see Guideline page 9)*. Furthermore, the principle of data processing (purpose limitation, data minimisation, storage limitation) as well as the technical-organisational measures must be observed *(see Guideline page 10 ff. and page 13 ff.)*. Please, keep in mind Ethics issues mentioned in the Guideline pages 23-30 and make sure to apply 'Ethics by Design'.

Collection of data in the Health Area	
Activities	**GDPR and Ethic Related Issues**
With in the DivAirCity project partners might undertake activities to collect data from citizens about their health and wellbeing. Possible activities might be: - Qualitative surveys and interviews - Group discussion to evaluate subjective dimensions of experience - Collection of health data with wearables for digital tracking of heart rate, number of steps and position-data (e.g. via a bracelet) - Collection of electrocardiogram-data via a chest strap (24-hour heart rate-variability using a long-term ECG)	If DivAirCity partners are planning such activities, the following must be considered: With these activities DivAirCity partners are not only collecting personal data in the meaning of the GDPR, but also special categories of personal data. Therefore, partners must consider more stringent data-protection safeguards. A declaration of consent form citizens is necessary *(see Guideline page 9)*. Furthermore the principle of data processing (purpose limitation, data minimisation, storage limitation) as well as the technical-organisational measures must be observed *(see Guideline page 10 ff. and page 13 ff.)*. Please, keep in mind Ethics issues mentioned in the Guideline pages 23-30 and make sure to apply 'Ethics by Design'.

Citizens activity formats	
Activities	**GDPR and Ethic Related Issues**
Possible activities that the DivAirCity partners might undertake regarding citizens activity formats: - Co-creative workshops (20-60 participants; analog/digital, depending on COVID) / Open Workshops - Stakeholder network meetings (20-30 participants; analog/digital, depending on COVID) / Workshops with stakeholders - Interview with stakeholders - Educational events (20-60 participants; analog/digital, depending on COVID) - Experimental workshops (small groups) / citizens science activities - Contests - Meet-ups	If DivAirCity partners are planning such activities, the following must be considered: For such citizens activity formats it will be necessary to maintain a list of contacts of participating citizens with names, emails, phone and address information. Thereby personal data in the meaning of the GDPR is collected so that a consent of those affected is required *(see Guideline page 9)*. Furthermore the principle of data processing (purpose limitation, data minimisation, storage limitation) as well as the technical-organisational measures must be observed *(see Guideline page 10 ff. and page13 ff.)*. Please, keep in mind Ethics issues mentioned in the Guideline pages 23-30 and make sure to apply 'Ethics by Design'.