AmsTErdam BiLbao cItizen drivEn smaRt cities

Deliverable 1.3: Data Management Plan

WP1, Task 1.5

Date of document

30/04/2020 (M6)

Deliverable Version:	D1.3, V.01
Dissemination Level:	PU[1]
Author(s):	DEUSTO

[1] PU = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Document History

This is the first version of deliverable D1.3 to be submitted in M6. We will update and complete it as many times as necessary, considering in the minimum to annual review and update.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Project Acronym	ATELIER	
Project Title	AmsTErdam and BiLbao cItizen drivEn smaRt cities	
Project Coordinator	Frans Verspeek ATELIER.EU@amsterdam.nl City of Amsterdam	
Project Duration	01/11/2019 – 31/10/2024 (60 Months)	
Deliverable No.	D1.3 Data management Plan	
Diss. Level	Public (PU)	
Deliverable Lead	DEU	
Status	x	Working
		Verified by other WPs
		Final version
Due date	16/04/2020	
Submission date	30/04/2020	
Work Package	WP1 - Project Management	
Work Package Lead	AMST	
Contributing beneficiary(ies)	All partners: AMST, COB, TEC, TNO, CAR, WAA, UAS, PSI, SEZ, BUD, MAT, RIG, COP, BRA, KRA, DEU, CEB, IBE, TEL, EVE, SPE, REP, POP, AMS, NET, DNV, GRE, CIV, ZIC, FRA	
DoA	A Data Management Plan (including a Data Protection Impact Assessment, DPIA) will be developed that consists of information on: the handling of research data during and after the end of the project, what data will be collected, processed and/or generated, which methodology and standards will be applied, whether data will be shared/made open access and how data will be curated and preserved (including after the end of the project). This will be updated halfway the project. The data manager will keep track of generated data sets and secures that it will fit to the procedures in the DMP. The Privacy Manager will be responsible for the DPIA and privacy issues during the execution of the project. DEUSTO will fulfil the roles of Data Manager and Privacy Manager, being responsible for the DMP including DPIA	

Date	**Version**	**Author**	**Comment**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

30/04/2020	01	Cristina Martín Andonegui	This is a live document that will be updated continually during the action and in the minimum once a year
30/04/2020	01	Tom Kober	Internal Reviewer
30/04/2020	01	Mark van Wees	Internal Reviewer
30/04/2020	01	Rudy Rooth	Non-official Internal Reviewer

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Tabe of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Abbreviations and Acronyms

Acronym	Description
CA	Consortium Agreement
DM	Data Manager
DMP	Data Management Plan
DMPR	Data Management Plan Responsible
DPIAO	Data Protection Impact Assessment Officer
EC	European Commission
FC	Fellow City
GA	Grant Agreement
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
LHC	Lighthouse City
LOD	Linked Open Data
ORA	Open Research Amsterdam
ORD	Open Research Data
PED	Positive Energy District
SCIS	Smart Cities Information System
WP	Work Package
WPL	Work Package Leader

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

0. Executive Summary

The EU-funded ATELIER project will demonstrate positive energy districts (PEDs) in eight European cities that will strive for sustainability and carbon neutrality. Amsterdam and Bilbao as lighthouse (LHC) but also Bratislava, Budapest, Copenhagen, Krakow, Matosinhos, and Riga are the fellow cities (FCs) aim at inspiring other European cities in replicating similar models that use PEDs as basic management unit for the implementation of energy transition strategies. Providing access to high quality data will facilitate the replication of the demonstrated solutions, the cooperation with other municipalities and the rapid uptake of results all along the European Union (EU).

This deliverable is targeting a consistent management of data all along the ATELIER data cycle (section 2) by defining two separate but interconnected sections: ATELIER Data Management Plan (DMP, section 3) and ATELIER Data Protection Impact Assessment (DPIA, section 4). The DMP provides a broad analysis of the data that will be generated, processed and/or stored by ATELIER partners. It provides a description of the methods to be used in terms of making ATELIER data findable, accessible, interoperable and reusable. The document also provides an explanation about the allocation of resources which includes the short/medium-term strategy and long-term strategy which assures ATELIER generated data would be preserve and accessible after the end of the project. Being ATELIER a smart city project, the seamless communication among the different city infrastructures, municipal services and citizens is crucial and keeps at the core of the project. Thus, making an efficient management of data and providing the mechanisms to deliver high quality standards is of vital importance.

ATELIER designs a DPIA plan that provides the tools and methods to implement the General Data Protection Regulation (GDPR) of the EU. The regulation tries to strike a balance between being strong enough to give individuals clear and tangible protection while being flexible enough to allow for the legitimate interests of businesses and the public. ATELIER not only provides the mechanisms to assess the risks regarding the use (or misuse) of personal data but it also provides methods to manage other ethic and security issues, as those related to the participation of volunteers, the participation (as beneficiary) of partners from non-EU countries or the security with respect to data management platforms. As basic DPIA tools, ATELIER foresees to track and continue filling the Data Protection Plans and the contact details of Data Protection Impact Officers of all the entities handling sensitive data or sensitive information.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

1. Introduction

The European Commission requires H2020 beneficiaries to accomplish with Open Research Data (ORD) pilot. The EC committed itself to running a flexible pilot on ORD that aims to improve and maximize access to and re-use of research data generated by Horizon 2020 projects. Accordingly, ATELIER is urged to endorse FAIR principles, making data findable, accessible, interoperable and re-usable.

1.1. The overarching data framework of ATELIER

ATELIER Data Management Plan (DMP) is designed on the idea of providing the necessary tools and mechanisms to promote suitable data handling procedures. The strategic model for energy transition (WP2) will be drawn through citizen and stakeholder participation (WP3 and WP7) that will pave the way for a rapid uptake of demonstrated solutions (WP4 and WP5). The monitoring and evaluation of all specific actions and in-city interventions (WP9) will be based on the analysis of data. On the top of that ATELIER plans to design a complete strategy for replication (WP6) and collaboration (WP8), as well as targeted set of dissemination and communication activities (WP10) that will champion the project outputs. The benefits, and therefore the commitment, of ATELIER partners to provide FAIR data is clear since that helps:

- ✓ encourage collaboration and replication avoiding duplication of efforts
- ✓ involve citizens and society improving transparency and public participation
- ✓ ensure quality of data processing at the monitoring and evaluation as well as other analytical work performed
- ✓ build on previous results and experiences, both within the ATELIER partnership and within EU
- ✓ speed up the innovation uptake and therefore, facilitate faster and greater development of markets

On the other hand, General Data Protection Regulation (GDPR) urge H2020 projects to assess and provide the security measures to manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data. The DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage those risks.

ATELIER will handle personal data at different chapters and with different purposes. Some examples include making a dynamic management of energy balances and therefore promoting prosumer behaviors (WP4 and WP5), working with volunteers in several activities promoting empowerment and cooperation (WP7), building up cities' transition labs based on citizen and stakeholder collaboration (WP3), etc. The protection of personal data will allow citizen and stakeholders to build close relationships with the municipalities, research organizations and industries because that would provide the trust and confidence they deserve.

1.2. Relation to other project tasks and deliverables

The Deliverable is part of Task 1.5: Data management and is linked with Task 1.1: Overall project planning & management and Task 1.4: Innovation management and market replication. It is further linked to Task 3.3 Monitoring the process of the PED Innovation Ateliers, Task 7.3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Citizens' behavior in system balancing and optimization and Task 9.2 Monitoring of progress for implemented measures in PEDs.

This deliverable is straightforwardly connected to D1.7 Open Access Research Data (also due M6). The deliverable D1.3 defines the methodologies and tools proposed to comply with a DMP in H2020 and DPIA accordingly to GDPR requirements, while the D1.7 analyses the mechanisms that allow the need to balance openness and protection of scientific information, fostering the open access to research data and project results. Both deliverables will keep a parallel progress and will work on the premise of making data 'as open as possible as close as necessary'.

1.3. Contributions and iterations with other partners

We have had multiple iterations with other partners, especially with cities (both LHCs and FCs), as well as with industrial partners (specially energy utilities, SPE and IBE), research entities working at the monitoring and evaluation (WP9, AUAS and PSI), the Work Package Leader (WPL) of the Citizen and Stakeholder Engagement (WP7, WAA), the WPL of the Cooperation with the SCC Community (WP8, AUAS) and the WPL of the Communication and Dissemination strategy (WP10, SEZ).

The Data Manager (DEU) organized a webinar the 14/02/2020 that was designed as an introductory seminar to explain the basic principles underlying DMPs and DPIAs under H2020 projects. The objective was to provide the tools and concepts that any entity participating in a H2020 action needs to know to guarantee appropriate data management, security and ethics. The participation of project beneficiaries was very significant (26 out of 30). The slides prepared for the session are shown in Annex 1. Both, the slides and the audio are shared to project beneficiaries[2].

[2] https://drive.google.com/drive/u/0/folders/1M7nRGczuDgtIsDKwewBJpGX6_M12lc6k

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

2. ATELIER Data Cycle

The ATELIER Data Cycle (Figure 1) includes both research data linked to publications as well as any other digital data generated during the project (Accordingly to GA, articles 29.2 and 29.3).

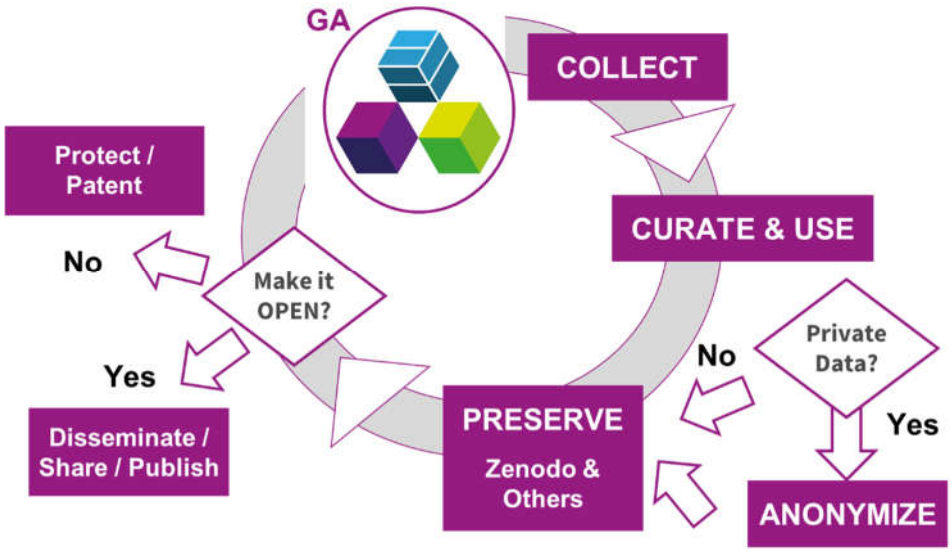


Figure 1: ATELIER Data Cycle

The ATELIER Data Cycle covers the full project and research cycle, it starts with the signature of the GA and the starting of the ATELIER action. As soon as the ATELIER team starts collecting data, we will gather and curate the data, and provide the means for anonymization and preservation. All the methods and tools that allow these steps are available at the Data Management Plan (D1.3). Once the data is preserved, data owner will decide upon making data open or not. The decision on making open the research data may take place not immediately after the generation. On the contrary, partners may delay the access to specific information (or data) making use of 'embargo period' that would be used to ensure the required protection or privacy methods

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

3. Data Management Plan (DMP)

The purpose of the DMP is to provide an overview of the main elements of the data management policy that will be used by the ATELIER project with regards to the methodologies and methods to be implemented.

ATELIER analysis data generated, processed and/or stored during the whole research data cycle. While this deliverable explains the most methodological aspects, D1.7 will reflect the current status of reflection within the consortium about the data that will be generated, collected, stored and processed. The ATELIER research data cycle includes four main chapters, data collection, data usage and curation, data preservation and data openness (D1.7, section 4). ATELIER works on a dataset by dataset basis by using ATELIER Data tracker and ATELIER template (D1.7, section 3.1). We provide most of the methodological aspects below.

3.1. Introduction

The purpose of the DMP is to provide an analysis of the main elements of the data management policy with regards to all the datasets that will be generated by the project. The DMP is not a fixed document but evolves during the lifespan of the project; in fact, it functions as a dynamic document of agreements. The DMP should address the points presented below on a dataset by dataset basis and should reflect the current status of reflection within the consortium about the data that will be generated, collected, stored and processed.

3.2. Data summary

3.2.1 Purpose of data collection and/or generation

In principle, publicly funded research data are a public good, produced for the public interest that should be made openly available with as few restrictions as possible in a timely and responsible manner that does not harm intellectual property. On this basis, the DMP intends to help researchers consider at an early stage, when research is being designed and planned, how data will be managed during the research process and shared afterwards with the wider research community. The benefits of a well-designed DMP not only concern the way data are treated but also the successful outcome of the project itself. A properly planned DMP guides the researchers first to think what to do with the data and then how to collect, store and process them, etc.

Furthermore, the planning of the data treatment is important for addressing timely security, privacy and ethical aspects. This way the research data are kept in track in cases of possible staff or other changes. The DMP can also increase preparedness for possible data requests and easy the collaboration among different partners. In short, planned activities, such as implementation of well-designed DMP, stand a better chance of meeting objectives and goals.

The process of planning is also a process of communication, increasingly important in a multi-partner research. The characteristics of collaboration should be accordingly harmonized among project partners from different organizations or different countries. The DMP also provides an opportunity to engender best practice with regards to e.g. file formats, metadata

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

standards, storage and risk management practices, leading to greater longevity and sustainability of data and higher quality standards.

Ultimately, the DMP should engage researchers in conversations with those providing the services. In this context, the DMP becomes a document in accordance with relevant standards and community best practice. Data should be shared, edited, and monitored among those contributing to the project. Releasing research data should follow legal, ethical and commercial terms and conditions. To serve the multiple purposes just described, the DMP is designed for easy digital exchange across a variety of applications. The best way to approach this in today's complex world of information technology is by adopting metadata standards (see D1.7, section 3.3.2) and field specific standards describing a data model of elements for the DMP.

3.2.2 RELATION TO THE OBJECTIVES OF THE PROJECT

ATELIER is aiming to demonstrate Positive Energy Districts (PEDs) within Amsterdam and Bilbao citizen-driven Smart Cities by validating innovative technological, business and governance solutions that would be scaled up and replicated all along the EU. In order to accomplish that, it is necessary to develop strategic visioning documents, integration of energy systems and ICT tools, new collaborative urban laboratories, as well as policy and legal framework conditions that will accelerate the acceptance of new energy models and the development of new markets and new business models.

The core of the project is embedded by PED Transition Labs or Ateliers (WP3) that will work on a quadruple helix methodology promoting the active collaboration of citizen, industry, research bodies and governance to pave the way towards new energy models that assume sustainability and carbon neutrality as ultimate objectives. These structures are established within Bilbao and Amsterdam Lighthouse Cities and follow the underlying ambition to become stable self-sustainable municipal structures. They are basic elements for the co-design and co-implementation of the PED demo site in Amsterdam (WP4) and PED demo site in Bilbao (WP5), where specific solutions such as the adoption of an increased shared of renewables, integration of different energy sources and storage methods, deployment of e-mobility solutions, development of new energy markets and, the promotion of smart and active collaboration with citizens among others are to be validated. The engagement with the general public will also be enforced by a wide set of activities specifically designed to balance the behaviors and attend different understandings (WP7). Both Lighthouse Cities (LHCs, Bilbao and Amsterdam) are working on their respective city vision 2050 (WP2) where strategic plans and roadmaps will be defined according to LHCs' own features and ambitions. Both, the innovation Ateliers (WP3) and city vision and planning (WP2), together with lessons learnt in the PEDs (WP4 & WP5) will be transferred and/or replicated in the six Fellow Cities (WP6). The monitoring and evaluation (WP9) will measure the impact of the measures performed in the PEDs and benchmark the outputs facilitating the visualization and communication of the project results. The cooperation with the SCC community (WP8) as well as the communication, dissemination and exploitation strategy (WP10) will enlarge the impact of the project, accelerating the uptake of the outputs and the generation of new markets.

In sum, ATELIER aims at setting up the systems and structures that will demonstrate PED as basic unit for energy transition. The rapid replication of ATELIER, first through FCs and then all along EU is a strong constant. That will be enormously facilitated by a healthy and consistent management of data that implements FAIR principles and favors openness of research data and research results.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

3.2.3 Specification of the origin and types of data generated and/or collected

ATELIER will measure the impact of the deployments installed in the PEDs of the LHCs which include deployment of specific infrastructures, integration of smart metering systems, sensing of buildings, integration of telecommunication systems, deployment of smart apps and visualization tools, etc. Data will also be gathered in relation to the participative mechanisms and collaborative strategies that aim at supporting citizens' behaviors towards new energy models. The progress of the project will also be measured with respect to the updates of legal frameworks, the number of new business models generated, the ambition and impact of the communication and dissemination activities, the number of meetings held, the resonance of the project in social media, etc.

In order to perform this, we will build define the status quo of LHCs and FCs gathering information and collecting data from:

1. strategic documents, indicators and plans already being used in LHCs and FCs that define boundary conditions and set up criteria for future scenarios

2. technology specific data of the infrastructure and innovative systems to be deployed in LHCs. That includes thermal and electrical energy systems, storage technologies, electrical vehicles performance, telecommunication infrastructure, data servers, etc.

3. stakeholders map including industrial partners, research institutions, clusters and associations, municipal service providers, local artists, schools and secondary educational centers, etc.

During the project lifespan of ATELIER we will generate a substantial amount of data both directly from the PEDs and the entire cities, and also as a result of data processing. That can be summarized as:

1. Data being directly measured from PEDs in Bilbao and Amsterdam and therefore verifies the deployment and validation of infrastructures at operational level

2. Outputs of questionnaires that will assess citizens' and stakeholders' behaviors and responses to participatory activities

3. Monitoring and evaluation data that will be expressed in terms of project indicators and results of holistic assessment tools (i.e. life cycle analysis) facilitating the extrapolation of measurements and the uptake of most effective solutions

4. Strategic documents, lessons learnt, deliverables and reports that will ease the replication and uptake of ATELIER methods, technologies and solutions

5. Software packages, methodologies (i.e. risk assessment), as well as dissemination material and other instruments that have facilitated the elaboration of methods for the deployment, evaluation and dissemination of ATELIER solutions.

3.2.4 Re-usage of data: to whom will it be useful?

The data already available at the LHCs and FCs will be largely increased all along the ATELIER project. The generated data will be re-used for several purposes and by several

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

stakeholders. The list will be updated along the project, while initial data have been identified as follows:

- Public authorities will make use of energy, mobility and environmental indicators to develop ambitious while realistic strategic plans. The transparency of information will increase the participatory opportunities and the social cohesion

- ESCOs, technology providers, etc. will be interested in data related to energy consumptions, energy generation rates of renewables, performance of storage systems, etc.

- Industry and service providers will make use of extensive data services of the municipality that would allow the identification of new business opportunities, the identification of increasing/decreasing demands, etc.

- Investors will use information about technology performance and maturity, payback rations of new solutions, etc. so that they can assess them and make better and more informed decisions

- Citizen would make use of data commons and specially of their energy bills and energy consumption profiles to interact more actively with the energy system and optimize their energy balances

- Civil organizations, neighborhood associations, etc. will keep an eye into citizen participation dynamics, impacts on their energy behaviors, acceptance of new solutions, pros and cons of innovative energy management systems, etc.

3.3. FAIR data

The FAIR principles precede implementation choices and do not necessarily suggest any specific technology, standard or implementation. Below, we explain the solutions and options that ATELIER will promote. During the course of the project, every dataset generated on the purpose of the project will be describe on a dataset by dataset basis using the ATELIER template (explanation provided at D1.7, section 3.3, and the template itself at D1.7, Annex 4)

3.3.1 Making data findable, including provisions for metadata

ATELIER pursues that any data and supplementary material use standard formats and identifiers so that it is easy to find. In this regard:

- We outline the discoverability of data by fostering the use of metadata standards[3] providing specific information for data related to engineering fields, social and behavioral science, research purposes, etc.

- We emphasize the quality of data and classify ATELIER datasets according to Tim Berners-L Classification[4] which encourage to move forward from text files (1 star) to linked open data (5 stars)

[3] http://rd-alliance.github.io/metadata-directory/
[4] https://5stardata.info/en/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

- We use unique identifiers for each dataset as *Dataset Number-WP Number-ENTITY Name* (see D1.7, section 3.3), and provide a data inventory (see D1.7, section 3.2) of all datasets and research data generated by ATELIER can be looked up, including document history

- We foster the use of a common language that will be generated naturally along the project. Common naming and acronyms are already arising such as: PEDs, LHCs, FCs, ateliers, upscale, replicate, archetypes, integration, smart tools, prosumers, etc.

- We will use clear versioning of all reports, documents and deliverables so their status and evolution is clearly recorded

- We foster the use of data standards according to regional consensus, national legislation, certification systems, etc. European or international standards such as ISO 50001:2018 Energy Management Systems or ISO 19115-1:2014 Geographic information are two examples.

3.3.2 MAKING DATA OPENLY ACCESSIBLE

ATELIER project aims at making data as open as possible, all the details about this policy are given in D1.7 (Open Access to Research Data). In this regard,

- we specify for each dataset whether it is open or not and explain the reasons why. All research data linked to open publications will be open by default (GA, article 29.2) as well as digital research data generated by the action (GA, article 29.3). The cities have also expressed their willingness to open as much data as possible to make information available to the general public and academia

- data will be made available by using open repositories. We use ZENODO as a common and 'by default' system to store all open ATELIER datasets. Institutional repositories from research centers and institutes as well as cities' open data services will be used (see section 3.4.3). ATELIER reports and deliverables will be accessible from the project webpage. Official reports will also be available at CORDIS[5].

- in general terms ATELIER data will be based on standard software in order to make it available to a broader audience. This aspect, will however, be specified for each dataset using the ATELIER template. In case that any further documentation is required to understand or make data accessible it is also to be provided

- in case of any particularities in sharing the data, those will be explained and justified

3.3.3 MAKING DATA INTEROPERABLE

ATELIER beneficiaries aim at generating interoperable datasets that will allow data exchange and reuse. All systems will be user friendly, well documented and unless otherwise specified openly accessible. ATELIER will follow established European metadata vocabularies, standards and methodologies.

[5] https://cordis.europa.eu/project/id/864374/es

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

On a dataset basis, ATELIER partners will specify any methods or software that might be necessary to access and manipulate the data. Those include:

- Data formats of spreadsheets, documents, geographical data, image, videos, etc.
- Methods or software needed to access the data and make it operable in other systems

3.3.4 MAKING DATA RE-USABLE

The possibility that a third person or entity makes use of a dataset entirely depends on the licensing conditions, as well as other intellectual property rights or permissions. ATELIER partners will be supportive to other stakeholders to decide which licensing or protecting options are the most suitable at each case. The use of Creative Commons[6] will be encouraged for digital creations (web page, contents of digital channels, etc.), other software might have specific (owner defined) terms of use.

In the Creative Commons framework, a decision tree is provided in order to help choose the most appropriated license (see fact sheet[7] *Which Creative Commons Licence is right for me?*). The five main questions to be answered are:

- Am I alright with other people copying and distributing my content without asking my permission every time?
- Am I ok with other people not recognizing my work?
- Am I ok with them changing and adapting the content?
- Do I want to limit how others can release their remixes?
- Am I right with other people making money out of their reuse of the content?

Depending on the answers a different license should be used. The details of every license shall be consulted at the Creative Common web page.

Copyright holders and creations will be protected in accordance with intellectual property rights (D10.6. IPR management report). Access permissions and restrictions will be identified indicating the list of partners involved, their roles, as well as the limitations given to each specific use and user. All research data generated by the action will be open by default (GA, articles 29.2 and 29.3) and therefore *the license should allow to freely used, re-used and redistributed by anyone – subject only, at most, to the requirement to attribute and share alike*[8].

3.4. Allocation of resources

The allocation of resources includes short-medium term and long-term strategies. The former defines who and how the expenses of making data fair will be covered as well as the data governance model which is already defined. The latter features the tools and methods that will allow the maintenance and preservation of data well after the project is finished.

[6] https://creativecommons.org/
[7] http://creativecommons.org.au/content/licensing-flowchart.pdf
[8] http://opendatahandbook.org/guide/en/what-is-open-data/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

3.4.1 FAIR DATA COSTS

ATELIER does not envisage to support cost of development of new data management platforms; however, it supports the cost of the use of open data systems. It also supports the integration of the data systems and the management of information, understood in wide terms, that is, all types of datasets that include configuration of systems, methodologies, instrumentation, photos, videos, newsletters, etc.

ATELIER partners have allocated a budget to make a consistent use and processing of data that supports FAIR principles. The openness of datasets to the general public is at the core of the project, and that is why we have specific chapters on making citizen aware about the availability and value of data: the ateliers (WP3) include as one of the tracks the data privacy, the engagement and participation (WP7) includes a chapter on the development of data commons, both demo sites (WP4 and WP5) include tasks making citizen participant of new energy markets, etc.

ATELIER fosters the public use of information through specific activities but also by providing public open repositories at the City Data infrastructure to facilitate the access and use of data (see section 3.4.3).

3.4.2 ATELIER DATA GOVERNANCE

ATELIER governance model (Figure 2) includes two differentiated levels designed in accordance with the requirements of the DMP and the DPIA.

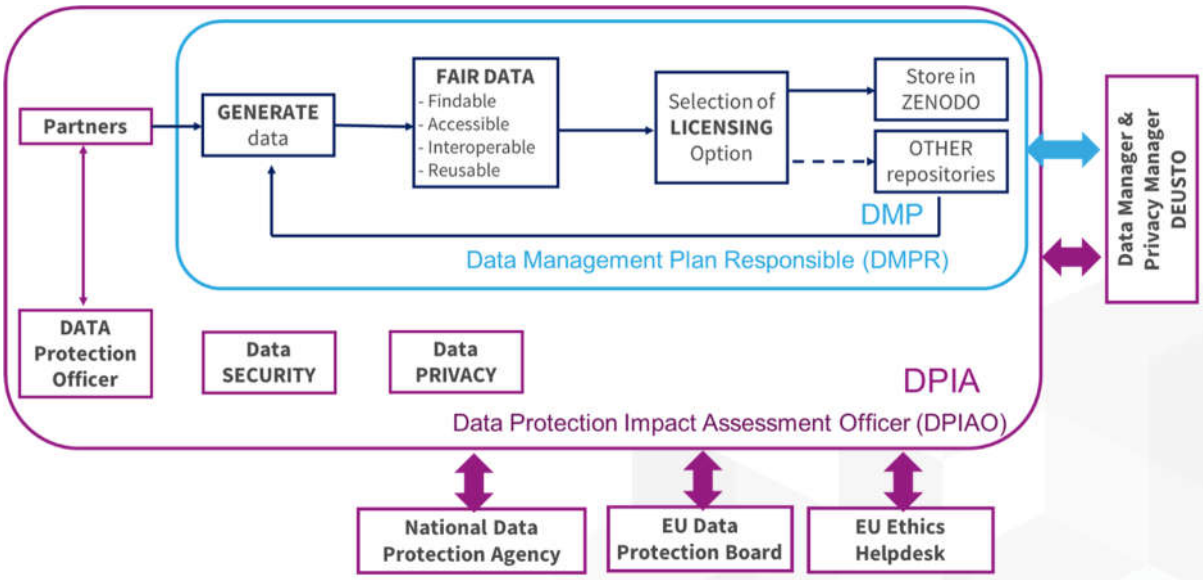


Figure 2: ATELIER Data Governance Model

1) **FIRST LEVEL**: Guarantees the quality of data with respect to FAIR principles

ATELIER DMP identifies a Data Management Plan Responsible (DMPR) per institution. This person belongs to the ATELIER team of this institution and will be responsible for:

- supervise the collection of data for the project
- prepare and collect consent forms (first draft available, see Annex 3)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

- discuss with the DPIAO (see below) about the internal procedures to collect, process and/or transfer personal data
- ensure that ATELIER datasets are FAIR
- facilitate the discussion about licensing
- prepare the dataset to be published (curate, anonymize, etc.)
- upload to ZENODO and any other public repository where the dataset will be preserved and/or made available
- complete the template from the Data Management Plan (see D1.7, section 3.3)

The DMPR will be aware of the progress of the project, be able to interact with all members of the ATELIER working team, keep constant communication with the ATELIER Data Manager and Privacy Manager (DEUSTO) and with the DPIAO.

2) **SECOND LEVEL**: Coordination of DPIA with DPIAOs

In the ATELIER DMP a Data Protection Impact Assessment Officer (DPIAO) is identified for all the benefiaries. This person belongs to the institution and is not necessarily linked to the ATELIER research team, but she/he is responsible for all the data privacy and data security issues of the entity. This person may already be defined at the institution or may be defined with the purpose of ATELIER. The DPIAO is in permanent contact with the Data Manager and Privacy Manager of ATELIER (Deusto) but also with the National Data Protection Agency, EU Data Protection Board and EU Ethics Helpdesk.

3.4.3 LONG-TERM PRESERVATION STRATEGY

Data will be made accessible for verification and reuse to various stakeholders through appropriate channels and repositories. Limited access and availability are to be indicated in the individual data descriptions (ATELIER data templates) and will be further developed within the project with the aim of achieving greater openness. Whenever research data is made available, it will be made available always in Zenodo (as common repository) and also (if appropriate) through any other thematic or institutional systems.

LHCs and FCs provide their City Portals as project repositories and work in line with ATELIER open data ambition to open as much data as possible in view of improving the transparency and public service to citizens. ATELIER will just reinforce this willingness and provide extra information about the PED performance. The open data portals of ATELIER cities are described below:

AMSTERDAM

Open Research Amsterdam (https://openresearch.amsterdam) is City of Amsterdam's digital platform for research, knowledge and innovation regarding Amsterdam and its broader Metropole region. The purpose of the open platform is to share knowledge, provide insights in working relations and create a platform for joint research and co-creation. The platform is mainly meant for civil servants of the City of Amsterdam and researchers of Knowledge Institutes in the region. A login name can be obtained via the City of Amsterdam.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

BILBAO

GeoBilbao (www.geobilbao.eus) is the municipal portal of the City of Bilbao. It is aligned with Bilbao Open Data[9] initiative whose main mission is to contribute, through the progressive publication of public data, to the development of economic sectors, to the promotion of administrative transparency and to the implementation of Smart Bilbao strategy. GeoBilbao was made open and available in 2012 and aims to provide geo-referenced data to citizens. For the moment, GeoBilbao allows the download and reuse of a total of 150 datasets or raw data sets on public transport, parking lots, public facilities, demography, tourism, economic-financial indicators, municipal budgets, tenders, contracting , works, environment, etc. GeoBilbao's functionalities are intended to facilitate the use of information and its analysis. To do this, 'Bilbao Open Data' uses free and free standards —such as CSV, XML, RDF, RSS, JSON, WMS and WFS—, which allow automatic processing of open data for public, private and commercial use. The open portal facilitates simple operations that include measuring distances, measuring areas, obtaining dimensions, drawing longitudinal profiles, extracting geocoders or transforming coordinates given in different standards. The initial number of data sets available (150) will be constantly increased and updated, always considering criteria of social utility, availability and economic and organizational sustainability.

BUDAPEST (HU)

The City of Budapest does not account with an Open Data City Portal, the public data generated by the municipality are published and available at the city webpage: https://budapest.hu. Data uploaded to the Information System of the Body is automatically published on the Budapest Portal, so it is cognizable for everybody without restrictions.

MATOSINHOS (PO)

Matosinhos has not any open city portal yet.

RIGA (LT)

At national level there is an open data platform (https://data.gov.lv/en) with a complete catalogue of data as well as searching and other functionalities. The City of Riga has not yet implemented an open city portal. However, Riga has several projects that have secondary impact on open-data and the digitalization of municipal services (see https://www.eriga.lv/). While the main goal of these projects is not a municipal open-data platform, the data is being prepared for opening if such political initiative should occur. Besides, Riga is working at several initiatives with respect to data interoperability and data-unification allowing open-data formats and geo-location centered formats (OData, CSV, WMS, XLSX, JSON, SHP, DOCX, XML, ZIP). Geo oriented data platform (formerly known as RIGIS / RIga Geographic Information System) was open until the autumn 2019 when municipality began transitioning from Microsystems based CAD/GIS software to ESRI GIS system.

Riga City Municipality provides 13 data sets out of a total of 371 open source datasets available at the state open data portal (data.gov.lv). These datasets include the register of inhabitants, municipal register of street addresses, registry of marriage, register of school & pre-school attendance, register of social, education, and sports services in the municipality, etc. Until the development of a municipal open portal, the national platform is hosting some municipal datasets.

[9] https://www.bilbao.eus/opendata/es/que-es-bilbao-open-data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

COPENHAGEN (DK)

”Københavnerkortet” (https://kbhkort.kk.dk/cbkort?&element=footer) is a publicly accessible, interactive map of Copenhagen that among other things shows the large construction projects of the city and the local plans. Users can click on any area of the city to access e.g. local plan documents and more details on various topics. Information concerning climate and energy can be found under the topic About the Municipality (in Danish: “Om kommunen”). Here the user can find information on administrative boundaries, city planning, climate adaptation, and municipal elections.

BRATISLAVA (SK)

The Bratislava Open portal (https://opendata.bratislava.sk/en/l) is focused on electronic services in the execution of self-governing functions of the city of Bratislava. It offers information and transaction services in Slovak and English. Transaction services create electronic submissions. These submissions shall have the same legal weight as classic letter submissions.

The City Portal includes hundreds of datasets about Bratislava, not only produced/owned by the municipality, but also publicly accessible data from various other sources, provided that they fulfill the data standards pursued by the city. Data visualization is facilitated through Microsoft PowerBi and GIS systems. The electronic services are categorized according to the categories of life situations and services. The philosophy of life situations is based on what a person experiences and what needs and duties life brings. This categorization of services emphasizes citizen orientation so that it can better orientate itself in the tangle of official concepts and procedures.

KRAKOW (PL)

The Municipal Spatial Information System of Krakow (MSIP, available on: http://www.msip.krakow.pl) is a little part of the City Portal, Magiczny Kraków or Magical Krakow (http://www.krakow.pl). Magical Krakow helps citizens, visitors and stakeholders participate in the life of the city, learn about the monuments and history of the city, establish business contacts, make investment offers, etc. MSIP website contains current and historical data about e.g. spatial planning, real estate market, transportation, demography. Information is provided in the form of accessible maps.

Another source of city information is Public Information Bulletin (BIP, available on: http://www.bip.krakow.pl). It is a Polish system of unified public records, which allows citizens to access public information. It contains reports, documents, strategies and legal acts provided by the President and Kraków City Council, as well as information about law, finance, city development. Part of BIP website is the ‘e-Office’ system (e-Urząd). It is a web-based platform, where citizens can send requests, opinions, complaint or submit an application.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 864374.

4. Data Protection Impact Assessment

4.1. Introduction

Data Protection Impact Assessment is directly linked to the EU legislation on personal data (Regulation 2016/6791, GDPR). Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (also referred to as Privacy Impact Assessment). A DPIA is a process designed to help manage the **risks to the rights and freedoms of natural persons resulting from the processing of personal data** by assessing them and determining the measures to address them[10].

GDPR provides a definition of personal data: '*Personal data means information relating to an identified or identifiable natural person. 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*'. Individuals are not considered 'identifiable' if identifying them requires excessive effort.

ATELIER, in response to the GA (articles 34, 36, 37 and 39), the CA (sections 9 and 10), and the EthSR (identifies requirements with respect to the use of personal data, the participation of non-EU countries, and the use of social media), implements a DPIA that includes the following chapters:

- Data Protection Plans
- Volunteers
- Security
- Non-EU countries

4.2. Data Protection Plans

Data Protection Plans (DPPs) will be submitted by all ATELIER entities processing personal data and will be used as basic element for Data Protection Impact Assessment. During the first DMP webinar (see section 1.2), ATELIER partners were proposed to consider the following decision tree in view of preparing (if necessary) their DPP (Figure 3).

[10] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

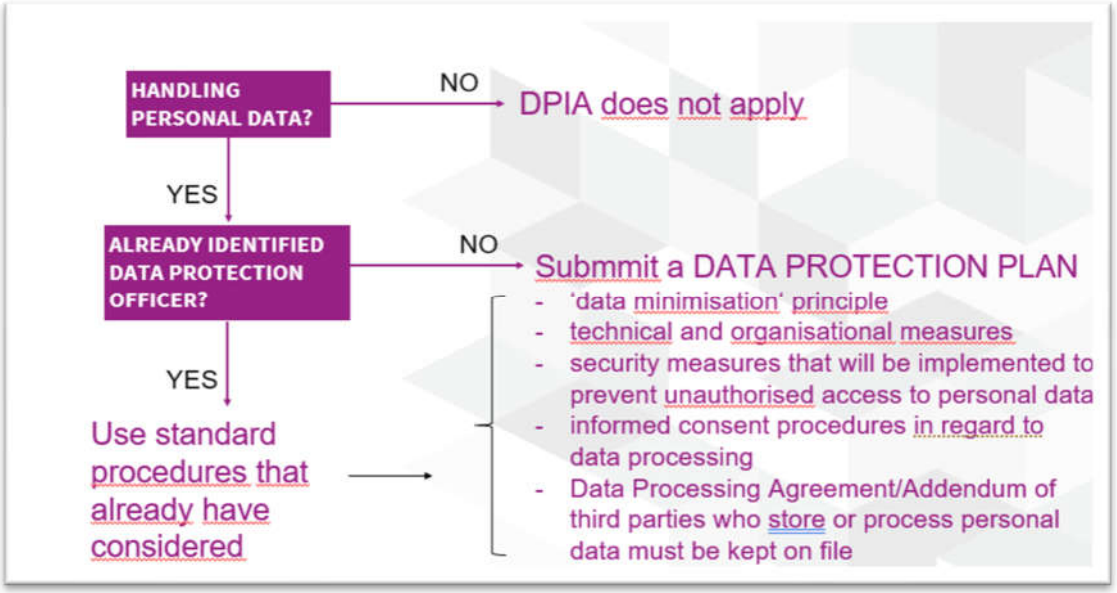


Figure 3: Decision Tree that ATELIER partners will follow for the preparation of DPPs

ATELIER DPPs will follow local, national, and EU regulations with respect to personal data processing. GDPR sets out the minimum features that a DPP should include (Article 35(7), and recitals 84 and 90):

- 'a description of the envisaged processing operations and the purposes of processing'
- 'an assessment of the necessity and proportionality of the processing'
- 'an assessment of the risks to the rights and freedoms of data subjects'
- 'the measure envisaged to:
- 'address the risks'
- 'demonstrate compliance with this regulation'

DPPs will be defined and kept on file prior to collecting, processing or handling any personal data, therefore ensuring that the Activity is consistent with data protection by design and by default principles (Article 35(1) and Article 35(10)). The plans will be integrals to all the activity of the company and would be dynamic and flexible accommodating to the requirements of ATELIER Data Cycle (section 2).

ATELIER Data Management Plan Responsible (DMPR) will also be responsible of ensuring that the DPPs are carried out. Therefore they become DPIA controllers accordingly to Article 35(2). DMPRs will work hand to hand with the Data Protection Impact Assessment Officers (DPIAO) and with any person handling personal data (processors, Article 35(2)). In case the management of personal data would endorse or be 'likely to result in a high risk to the rights and freedoms of natural person (Article 35(1), see III.B.a)' supervisory authorities shall be consulted, i.e.: National Data Protection Agency, EU Data Protection Board, EU Ethics HelpDesk (as external consultancy body).

The ATELIER partners who have already confirmed that they will generate or handle personal data are:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

- **IBERDROLA (IBE)**: gathers electrical consumption that reflects domestic activities and habits and implements smart grid in Bilbao PED. The DPP of Iberdrola is open and accessible from IBE website[11]. Iberdrola designates Alfonso Menchen as Protection Delegate for Spain and María Teresa Rodríguez de Tembleque as Global Data Protection Coordinator. Those names are also provided at ATELIER Governance file (D1.7, section 3.1.6).

- **SPECTRAL**: establishment of local energy communities and development and installation of smart (micro)grids in Amsterdam PED. The DPIAO at Spectral is Stephen Donnely, also CEO of the company (see Governance.xls, D1.7, section 3.1.6). Spectral is working on the DPP that will be finished and reported before start collecting personal data. Spectral already has defined the phases and steps this plan will have (see Annex 2).

These entities will collect information about energy consumption and be directly implied in the development of Bilbao and Amsterdam smart grids. They are already in contact with the respective LHCs and work in collaboration with other partners. In the current status of the project, they do not consider sharing personal data with any other partner. On the contrary, they intent to anonymize any customer using ad hoc methods that will largely depend on the specific type and format of data. In case, they see the necessity of sharing any personal data, the DPIA will be updated consequently and confidential agreements between the partners involved will be signed.

The **DE WAAG SOCIETY** WPL (WP7: Citizen and stakeholder engagement) will lead the mapping of stakeholders (T7.1) and organize activities to work with volunteers. It might be that WAAG retrieves information from participants in the form of questionnaires, surveys, etc. They are working on a Data Privacy Policy that would be ready before conducting any activity that implies the use of personal data. Further versions of the ATELIER DMP might identify more partners that will handle personal data and will report about the procedures to be used.

4.3. Volunteers

ATELIER keeps at a very central part the interaction with participants and stakeholders through a trans-disciplinary collaboration. We foresee the participation of volunteers all along the project and with respect to all the WPs, especially at all the workshops carried out in WP3 and all the activities designed to engage with the stakeholders and citizens (WP7).

The methods of recruitment will be ad hoc designed for each of the participative session. The organizing entity (ATELIER partner) will present the recruitment procedure and keep it on file. The volunteers will be informed about the context and purpose of the participatory activity, their role as volunteer, the data we might be gathering from this activity, etc. A very preliminary draft of the informed consent forms to be used during the project is shown in Annex 3 and made available at the Shared Disk (see D1.7 section 3.1.1).

11 https://www.iberdrola.com/wcorp/gc/prod/en_US/corporativos/docs/personal_data_protection_policy.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

More detailed requirements and documentation will be generated before the start of any activity involving participation of humans as subjects of the study, while fully operating within local, national, and EU regulations. These forms will be detailed and tailored to the individual activities, objective public and LHC or FC. They will use the official language of the country/city where the activity takes place and include local context specific aspects referring to the relevant regulations on data protection and/or other legislation if applicable.

For all applicable physical meetings and consortium events we will inform participants that pictures will be taken, and participants will have to actively consent to, with an option to opt out from pictures (or any other multimedia material) being used in project specific communication. It also concerns photographic evidence of events, demonstrations, etc. that are to be done throughout the project and may be needed for deliverables (internal or official) and reports. This will also be specially considered with WP10 on communication and dissemination and WP8 on cooperation with SCC community.

4.4. Security

Security measures are related to a wide spectrum of ICT systems that ensure the collection, communication, processing and storage of data. They involve multiple partners that will work together to fulfill the project tasks and milestones. Some clear examples are:

- The deployment of Smart Grids and Energy Management System in Bilbao (WP5) which involves COB, CAR, DEU, TEL, IBE, EVE, and the citizens

- The deployment of Smart Grids and Energy Market System in Amsterdam which involves SPE, GRE and FRA, and the citizens

- The design and generation of Energy Data Commons (WP3, WP7) that involves in the minimum COA, COB, WAA, AMS, DEU, TEC, AUAS, EVE, SPE) and the citizens

- The connectivity and functionally of Bilbao data platform as main information repository for the design of City Vision (WP2), the implementation of smart iteration tools (WP5), the monitoring and evaluation of ATELIER's PED measures (WP9), etc.

- The connectivity and functionally of Amsterdam data platform as main information repository for the design of the City Vision (WP2), the implementation of energy markets (WP4), the monitoring and evaluation (WP9), etc.

The beneficiaries will implement technical and organizational measures to ensure privacy and data protection rights in the project. All ICT systems to be developed will be designed to safeguard collected data against unauthorized use and to comply with all national and EU regulations. EU guidelines on general standards will be followed, e.g., ISO/IEC 27001 and 27002 (Code of practice for information security management), to ensure confidentiality, integrity, and availability. It will additionally include the Directive on security of network and information systems ('Cybersecurity directive', NIS-Directive 2016/1148) on the security of critical infrastructures and the ePrivacy Directive 2002/58, as well as European Union Agency for Network and Information Security (~) guidance. Engineering best practices and state-of-the-art data security measures will be incorporated as well as GDPR considerations, and respective guidelines and principles. Ultimately, each partner is responsible for their own information security in its respective IT/data systems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

ATELIER LHCs and FCs have their own data protection routines established in their existing operations and in their development and test activities of the project. They are responsible to establish compliance with GDPR and other data protection and security regulations in accordance with the local, regional and national law.

CITY OF AMSTERDAM

The Data Management Policy of the Municipality of Amsterdam responds to the *May 25, 2018, the General Data Protection Regulation (GDPR / AVG)* and applies to all processing of personal data. This European legislation has direct effect in the Netherlands. The AVG Implementation Act in the Netherlands additionally applies to those matters that must be regulated nationally. The Privacy Statement of the Municipality designates the Data Protection Officer (also reported at ATELIER Data Governance D1.7, section 3.1.6).

The Municipality of Amsterdam attaches great importance to good protection of personal data. The City of Amsterdam also takes appropriate organizational measures to properly protect personal data against misuse, loss, unauthorized access and processing. Thus ensuring:

- Processing of personal data properly, lawfully and transparently, on the basis of a legal basis for processing personal data,
- Collection and usage of personal data only for a specific and clearly defined purpose and only uses the personal data for the purposes for which they were collected or for the (compatible) purposes for which they are further processed, including scientific and historical research, archiving in the public interest and statistical purposes,
- Only to process the personal data necessary for the purpose,
- The personal data is correct and updated if necessary,
- Not to store personal data longer than necessary. The necessity is related to the purposes to which the relevant personal data refer to or as long as this is necessary for compliance with legal obligations, for example for archiving or statistics,
- To take appropriate organizational and technical measures for the protection of personal data

For the performance of the duties and responsibilities of the city, we work together with partners outside the organization of the municipality of Amsterdam. This can be other governmental bodies, but sometimes also private parties. In certain cases, we share personal data with those organizations. When we exchange personal data with other parties, we make agreements about this that are in line with applicable laws and regulations. When personal data is provided to parties outside the European Economic Area (EEA), this will be in accordance with the requirements of the law, such as making appropriate agreements about the level of data protection in that country.

CITY OF BILBAO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

The legal framework of Bilbao Open Data[12] complies with existing legislation at European, national and municipal level. At EU level, Bilbao fulfills as general references the *Directive 2003/98 / EC of the European Parliament and the Council of 17 November 2003 on public sector information* and the *Directive / 2013/37 / EU of the European Parliament and of the Council of June 26, 2013, amending Directive 2003/98 / EC on the reuse of public sector information*. Bilbao follows the Spanish regulation *Law 37/2007, of November 16, on the reuse of public sector information* that transposes the European Directive 2003/98 / EC and the *Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights*. With respect to transfer of Data Privacy Policy[13], sensitive data processing will only be proceeded if necessary and for the fulfillment of a mission carried out in the public interest or in the exercise of public powers (RGPD 6.1). At this respect Bilbao follows its competences based on *Spanish Law 7/1985, of April 2, Regulating the Bases of the Local Regime* and *Law 2/2016, of April 7, on Local Institutions of the Basque Country*.

At municipal level, *The Open Government Alliance* (*Alianza para el Gobierno Abierto*) was launched in 2011 as an international platform for domestic reformers committed to holding their governments accountable, more open, and improving their responsiveness to their citizens. Although the Alliance does not constitute a legislative or normative mandate, it has become the most recognized international reference. The scope of the Alliance includes open data initiatives, but also includes the other aspects of Open Government, thus constituting a broad framework of implementation. The Data Protection Plan of Bilbao is available online[13] as well as the contact (email) of the Data Protection Officer (Delegado de Protección de Datos) (see ATELIER Data Governance D1.7, section 3.1.6).

BUDAPEST (HU)

The City of Budapest complies with the national law *Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information* that establishes the fundamental rules for data processing activities with a view to ensuring that the right to privacy of natural persons. The scope includes any data management procedure which is related to personal information as well as data of public interest in view of guaranteeing the privacy of individuals as well as fostering the process of making public affairs transparent. Other important national laws that Budapest City guarantees are the *Act L of 2013 on the Electronic Information Security of Governmental and Municipal Bodies* and the *Act LXII of 2012 on the Recycling of Data of Public Interest*. At municipal scale, ATELIER will fulfill the *Joint Instruction 1/2019 (I. 3.)* on the data privacy of the Municipality of Budapest, the data security and the procedures of disclosure of data of public interest. The municipal instruction applies at all the internal organizational units, as well as all of its employees and the City Council of Budapest and its Committees, Representative and Non-representative Members who perform any activity related to administering, storing or providing either personal data or data of public interest, or preparing documents (proposals, handouts, reports, etc.) containing such data. The Privacy Policy is available at: http://einfoszab.budapest.hu/list/adatkezelesi-tajekoztatok

[12] https://www.bilbao.eus/opendata/es/marco-legal-existente

[13] https://www.bilbao.eus/cs/Satellite?c=Page&cid=3000106346&language=es&pageid=3000106346&pagename=Bilbaonet%2FPage%2FBIO_contenidoFinal&pageid=1272994181655

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

MATOSINHOS (PO)

The City of Matosinhos (Câmara Municipal de Matosinhos, CMM) allows the access of personal documents of citizens and companies only to some employees accordingly to GDPR principles and is therefore not freely accessible. Access to employees' personal data is also limited to some human resources technicians. GDPR is regulated by the Law number 58/2019 and Law 59/2019, both approved on the 8th of August by the Assembly of the Portuguese Republic.

RIGA (LT)

Riga City Municipality is fully compliant with the General Data Protection Regulation (EU) 2016/679 of the European Parliament and the European Council of 27 April 2016 (further – GDPR). On the National level the "Law on Personal Data Processing" has been adopted on 21 June 2018 with a purpose to define legal preconditions for setting up a system for the protection of personal data of a natural person at a national level, determining the competence and basic principles of operation thereof, as well as regulating operation of data protection officers and provisions of data processing and free movement. (Law is available online in English): https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law.

On the municipal level on 4 April 2016 the city has adopted municipal regulations "Rules and Procedures of the Security Centre for Data Protection and Information Technology of the Riga City Council" aimed to coordinate and supervise safety and compliance of the personal data protection and municipal information and communication technologies/services with the requirements of binding regulatory framework at the municipality – city administration and all municipal structural units (departments, directorates, municipal agencies, enterprises, services providers, etc.).

The regulation enforces compliance with GDPR requirements and requires each municipal unit to assign their data managing officer. The role of data security is uniformly assigned to the Security Centre for Data Protection and Information Technology of the Riga City Council, also referred as the Data Protection Centre (DAC). The institution has elaborated detailed protocols aimed to ensure compliance of all municipal processes with the GDPR. The Head of the DAC is authorized as the Data Protection Manager of the municipality. A Data Protection Officer (DPO) is appointed for all municipal structural units who acts in-line with the GDPR and ensures compliance of data management with National legislation and municipal regulations.

COPENHAGEN (DK)

Copenhagen Municipality is obligated to follow the national rules regarding data protection. The Danish Data Protection Agency (in Danish: Datatilsynet[14]) is the independent authority that monitors compliance, handles complaints, as well as provides guidance and advice. This also includes provision of e.g. templates for data processor agreements (see Annex 4). Within Copenhagen Municipality it is the City Data Department that is the main data handling department.

[14] https://www.datatilsynet.dk/generelt-om-databeskyttelse/lovgivning/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

BRATISLAVA (SK)

Bratislava Municipality endorses the Slovak law *18/2018 Z.Z.*[15] *– Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov* that translates GDPR requirements into national legislation.

With respect to security issues, Krakow introduced the Information Security Policy of the City of Krakow in 2010, under the Ordinance of the Mayor of Krakow No. 958/2010 regarding the introduction of the Information Security Management System at the Municipality of Krakow. Implemented system is certified according to the requirements of ISO 27001. Personal data is processed in order to provide services by the City of Krakow. This is realized in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

At municipal scale, the Internal Directive 8/2018 on Data Protection ensures the GDPR implementation and translation into municipal legislature and the adoption of an Internal Directive 9/2019 on Data Policy that regulates the rules for the collection, generation, monitoring, sharing and manipulation of data sets (including geospatial data sets) and the process of publishing data on the open data portal of the Capital City of the Slovak Republic Bratislava. The Data Officer is Mgr. Michaela Peťovská (contact details available at the Data Governance.xls).

KRAKOW (PL)

Krakow introduced the Information Security Policy of the City of Krakow in 2010, under the Ordinance of the Mayor of Krakow No. 958/2010 regarding the introduction of the Information Security Management System at the Municipality of Krakow. Implemented system is certified according to the requirements of ISO 27001.

Personal data is processed in order to provide services by the City of Krakow. This is realized in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

4.5. Non-EU Countries

ATELIER includes a non-EU partner, Paul Scherrer Institute (PSI) located in Switzerland. PSI is the leader of WP9 (Monitoring and evaluation) and participates in WP1 (Coordination), WP2 (City Vision and Planning), WP3 (Transition Labs) and WP10 (Communication and Dissemination). In case personal data would be transferred to Switzerland, PSI will confirm that such transfers are in accordance with Chapter V of the GDPR 2016/679. In case any personal data would be generated in Switzerland, the procedures will follow the legal procedures of at least one EU Member State and will be transferred back to EU (if necessary) accordingly to Swiss laws.

The Data Policy on Research Data (in English) and Information Security Procedures (in German) of PSI are documented (and kept on file), and are aligned with GDPR which would

[15] https://www.zakonypreludi.sk/zz/2018-18

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

facilitate any operation. During the course of the project and in case any transfer of personal data would be required, the corresponding procedures will be further explained and submitted as part of D11.1: POPD - Requirement No. 1 and D11.2: NEC - Requirement No. 2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

5. Conclusion

This deliverable constitutes the first Data Management Plan of ATELIER. It is delivered in April 2020 and will be regularly followed up and advanced with the consortium members. The next official delivery of D1.3 will be in M33. The data manager (DEUSTO) will keep the responsibility of keeping this live document updated, and also the tools and instruments that ensures its correct performance.

Deliverable D1.3 is directly linked to deliverable D1.7 (Open Access to Research Data). These documents are closely linked and strike for an effective and high-quality data management performance. It might be that some methodological aspects are being changed or updated according to project necessities and partners requirements. As basic elements for the Data Management Plan, ATELIER accounts with a set of shared resources (with all project partners) that include these deliverables, the records and slides of the webinars, the data inventory (D1.7, section 3.2), and the dataset templates (D1.7, section 3.3). With respect to DPIA, each partner (beneficiary) keeps the responsibility of preparing and keeping on file the Data Protection Plans as well as the consent forms to recruit and work with volunteers, or any other document required by the GDPR. DEUSTO as Privacy Data Manager will support and provide help.

The link between deliverable D1.3 and D1.7 will be maintained all along the project, in a manner that both documents are maintained and developed consistently. Any change in one deliverable affecting the other one will translate into immediate amendments of the other deliverable. The underlying idea (to be modified if necessary) is to keep D1.3 as more methodological deliverable and D1.7 as main working document.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Annexes

Annex 1: Slides prepared for the webinar of the 14/02/2020 (ATELIER DMP 1st webinar)

Annex 2: The phases and steps that DPIA of Spectra will include

Annex 3: Draft of ATELIER Consent Form

Annex 4: Templates of Data Processor Agreements at the City of Copenhagen

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

D1.3 Annex 1

Slides prepared for the webinar of the 14/02/2020
(ATELIER DMP 1st webinar)

AmsTErdam BiLbao cItizen drivEn smaRt cities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

DATA MANAGEMENT PLAN – WEBINAR

Cristina Martín & Cruz E. Borges

UNIVERSITY OF DEUSTO

AmsTErdam BiLbao cItizen drivEn smaRt cities

atelier

Positive Energy Districts

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Purpose of the webinar

Provide the tools and concepts that any entity participating in a H2020 action needs to know to fulfill the EU policy and requirements with respect to data management, security and ethics

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Agenda

- Data Management Plan in H2020 projects
- Data Protection Impact Assessment
- Open Access Research Data
- How can we start?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

DATA in H2020 projects

Nearly everything is data!

Datasets but also: reports, questionnaires, software, video/pictures, publications, etc.

FORMAT

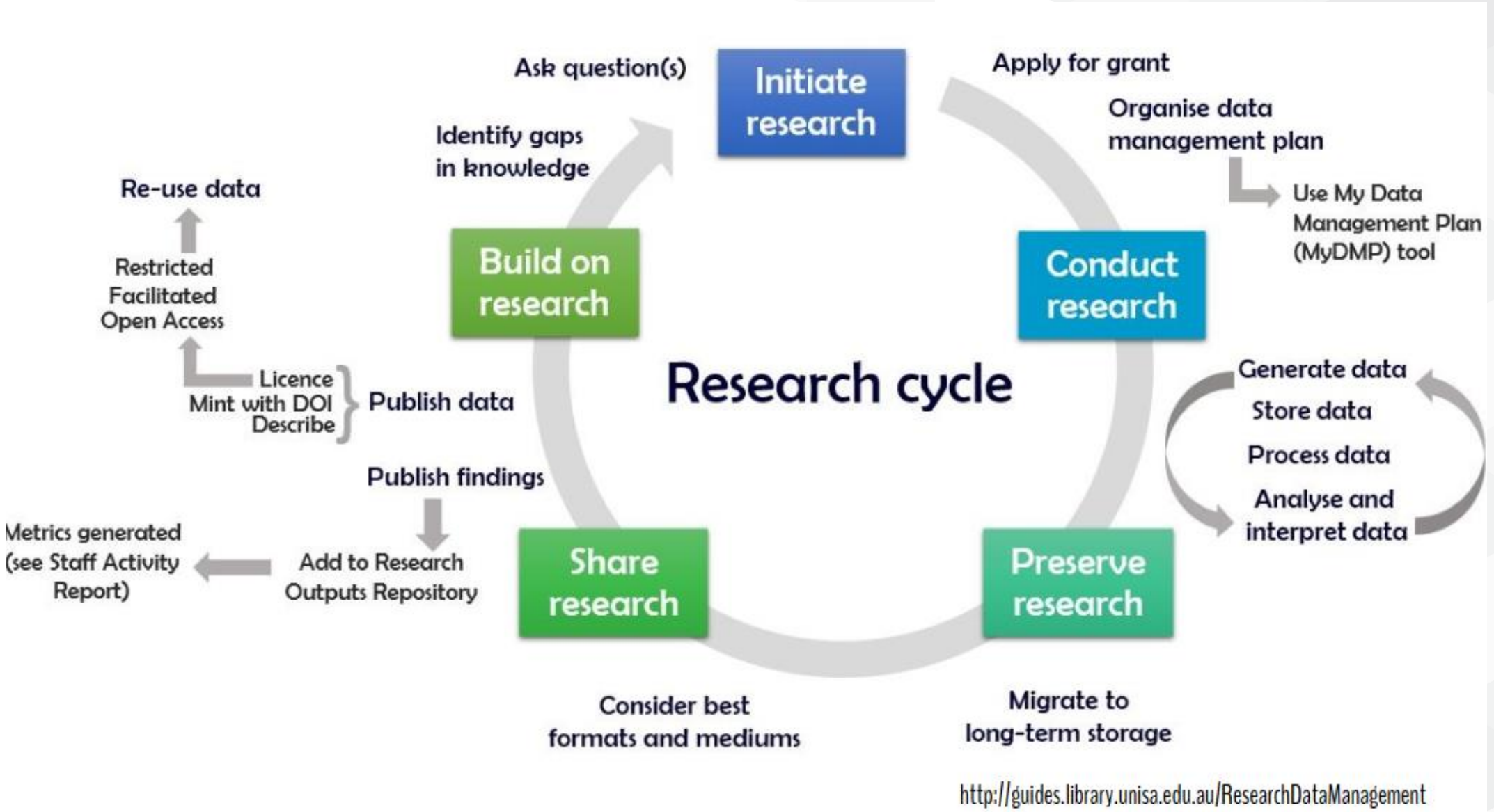
- Text
- Figures
- Multimedia
- Estructured data
- Software

ORIGEN

- Experimental
- Simulated
- Observed
- Derived or calculated
- Reference

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Research Data Management



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

H2020 requires...

- Data Management Plan (DMP)

It will be a live report that detailing *what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved*

ATELIER, D1.3. Data Management Plan (M6, M33), updated annually

- Data Protection Impact Assessment (DPIA)

It includes the chapters referring to*: security, ethics and privacy*. In ATELIER the DMP (D1.3) includes the DPIA

- Open Access Research Data

All information about Research Data and Publications and whether they will become open or will be protected to be exploited

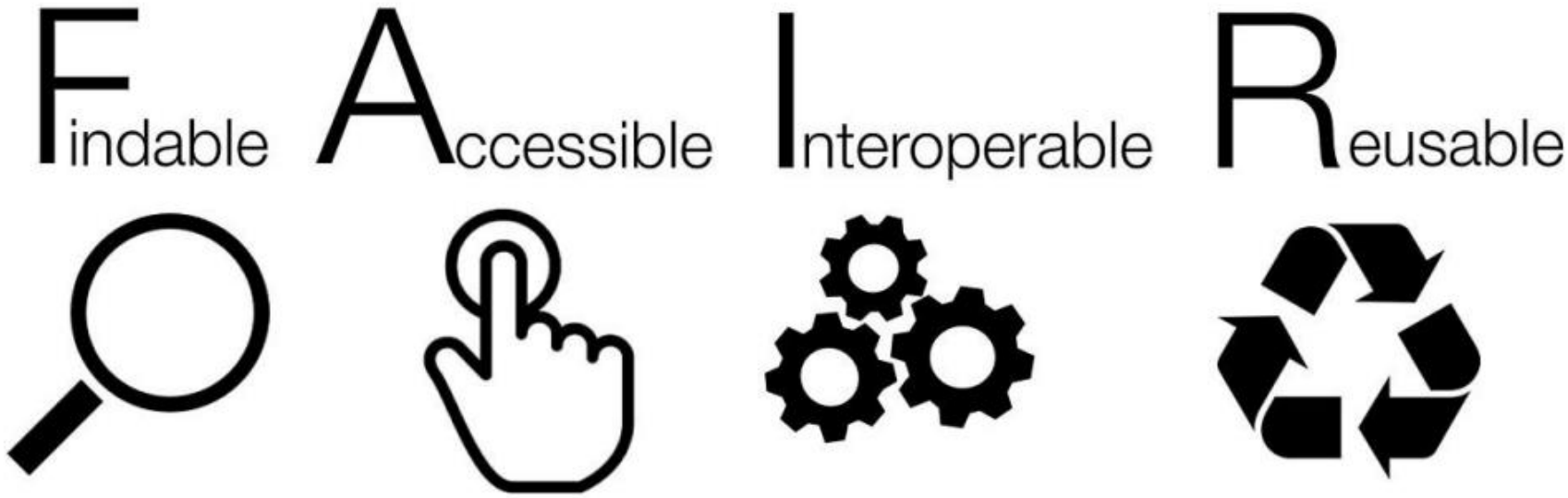
ATELIER, D1.7 Open Access Research Data, updated annually

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

DATA MANAGEMENT PLAN

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

DMP: FAIR data principles



CC BY-SA SangyaPundir
https://commons.wikimedia.org/wiki/File:FAIR_data_prirciples.jpg

https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

FAIR principles

FINDABLE

Data and supplementary materials have sufficiently rich metadata and a unique and persistent identifier

ACCESIBLE

Metadata and data are understandable to humans and machines. Data is deposited in a trusted repository

INTEROPERABLE

Metadata use a formal, accessible, shared, and broadly applicable language for knowledge representation

REUSABLE

Data and collections have a clear usage licenses and provide accurate information on provenance

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Quality of Data

http://5stardata.info/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Repositories

- ZENODO → OpenAir

Zenodo is a general-purpose open-access repository developed under the European OpenAIRE program and operated by CERN

- EU Smart Cities Information System (SCIS)

ATELIER project already published. Specifically designed to share data with other Smart City projects

- Other institutional repositories
  - City open data portals
  - Openstreetmaps
  - Etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

DATA PROTECTION IMPACT ASSESSMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

DPIA

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[4] by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)[5]. In other words, **a DPIA is a process for building and demonstrating compliance**.

Regulation 2016/6791 (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA2), as does Directive 2016/6803

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

What is ‘Personal Data’?

Personal data’ means information relating to an identified or identifiable natural person.

‘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 (art. 2(a) EU General Data Protection Regulation (GDPR)’.

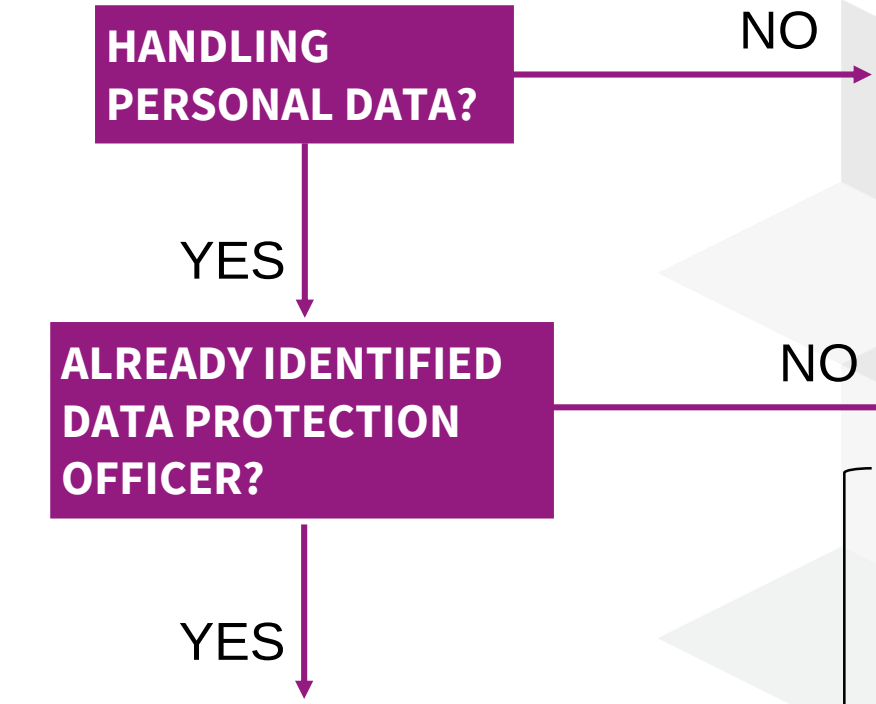
Individuals are not considered ‘identifiable’ if identifying them requires excessive effort.

Completely anonymised data does not fall under the data privacy rules (as from the moment it has been completely anonymised).

H2020 – Ethic Self Assessment

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No.864374

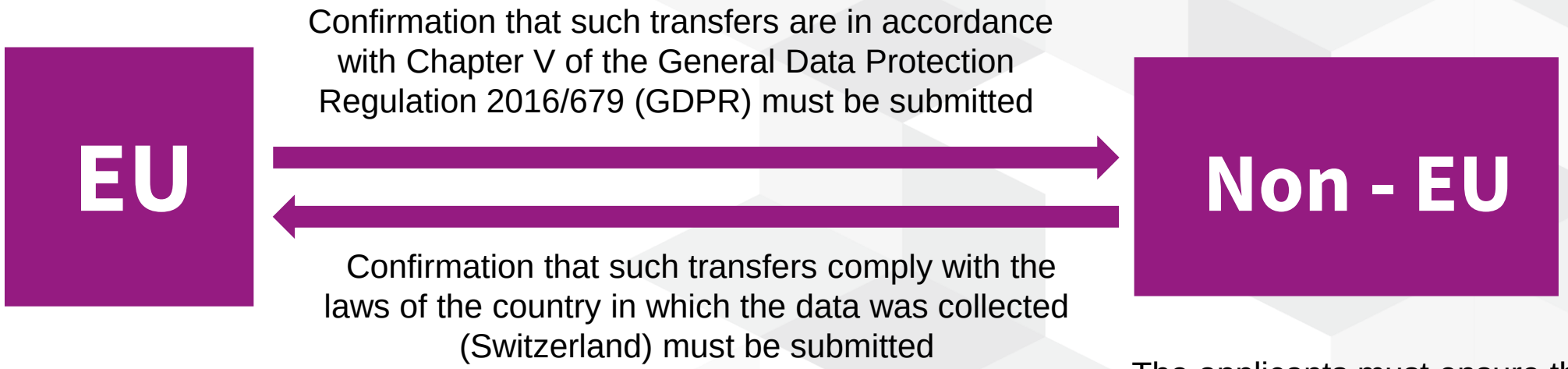
DPIA



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Ethics related Data issues

- Transference of Personal Data to non-EU countries



The applicants must ensure that the research conducted outside the EU is legal in at least one EU Member State

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Volunteers and the Data

- Recruitment and consent procedures will be provided explaining the details about:
  - The procedures and criteria that will be used to identify/recruit research participants.
  - The informed consent procedures that will be implemented for the participation of humans.
  - Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants).
  - If children/minors are to participate, justification for their participation and the acquirement of consent of their legal representatives will be provided

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Security

EU regulations

Relevant EU standards, e.g., **ISO/IEC 27001 and 27002** (Code of practice for information security management), to ensure confidentiality, integrity, and availability. It will additionally include the Directive on security of network and information systems (‘**Cybersecurity directive’, NIS-Directive 2016/1148**) on the security of critical infrastructures and the **ePrivacy Directive 2002/58**, as well as **European Union Agency for Network and Information Security (~) guidance**.

National Regulations

For the moment, we will account for Data Regulations of main entities generating data:

- Lighthouse Cities: National, regional and municipal laws
- Follower Cities: IDEM

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No.864374

Platforms and security

Tag Type	Description	Security Features	Access Credentials
Blue	Public	Clear storage, Clear transmit	Open
Green	Controlled public	Clear storage, Clear transmit	Email- or OAuth Verified Registration
Yellow	Accountable	Clear storage, Encrypted transmit	Password, Registered, Approval, Click-through DUA
Orange	More accountable	Encrypted storage, Encrypted transmit	Password, Registered, Approval, Signed DUA
Red	Fully accountable	Encrypted storage, Encrypted transmit	Two-factor authentication, Approval, Signed DUA
Crimson	Maximally restricted	Multi-encrypted storage, Encrypted transmit	Two-factor authentication, Approval, Signed DUA

http://datatags.org/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

OPEN RESEARCH DATA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Open Research Data Pilot in H2020

In Horizon 2020 the Commission committed itself to running a flexible pilot on open research data (ORD Pilot). **The ORD pilot aims to improve and maximise access to and re-use of research data generated by Horizon 2020 projects**. It takes into account the need to balance openness and protection of scientific information, commercialisation and IPR, privacy concerns, security as well as data management and preservation questions.

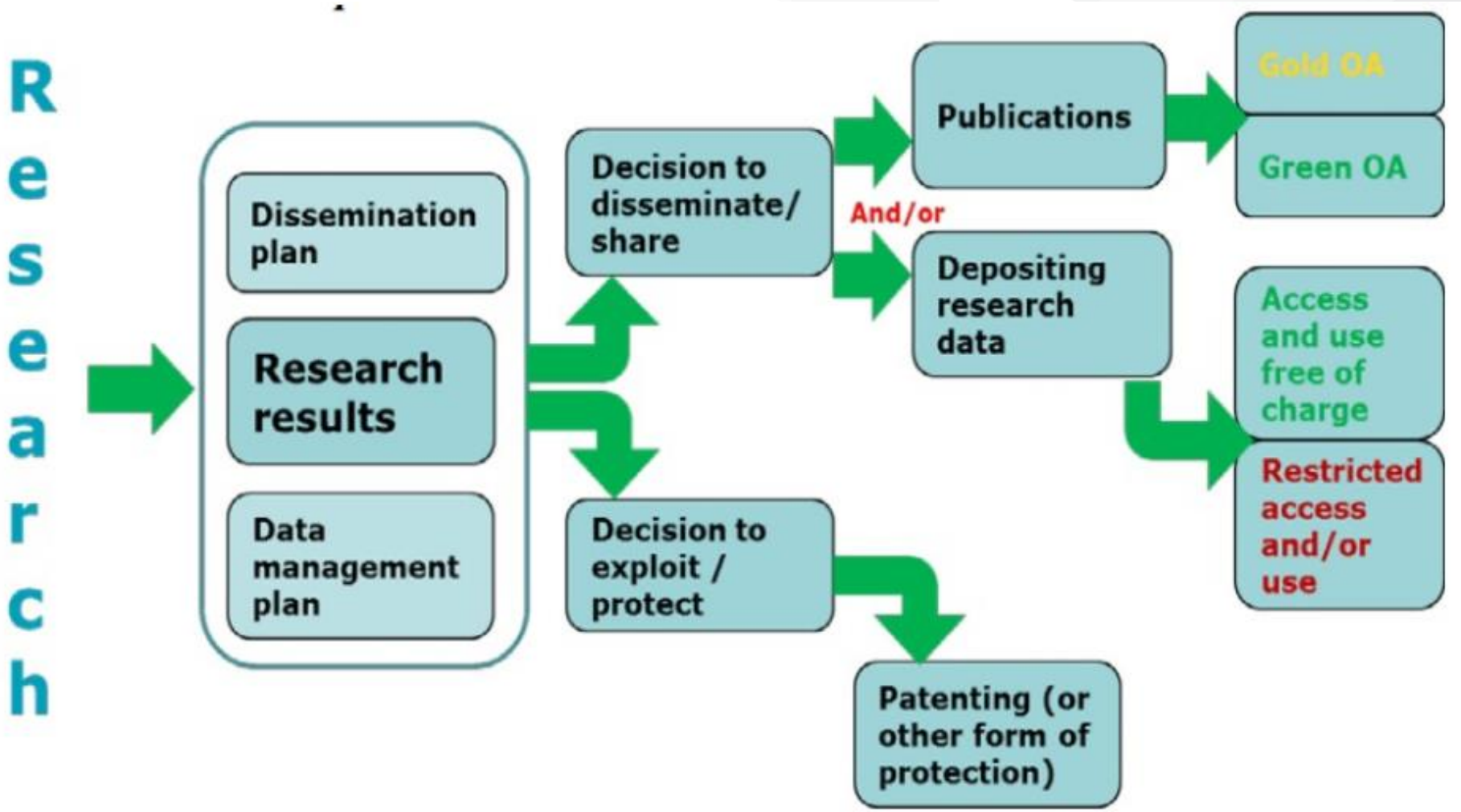
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

⚠ Please note the distinction between open access to scientific peer-reviewed ***publications*** and open access to research ***data***:

- **publications** – open access is an *obligation* in Horizon 2020.
- **data** – the Commission is running a flexible pilot which has been extended and is described below.

From: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374



Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020
http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

⚠ Participating in the ORD Pilot does not necessarily mean opening up all your research data. Rather, the ORD pilot follows the principle "**as open as possible, as closed as necessary**" and focuses on encouraging sound data management as an essential part of research best practice.

From: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Misconceptions of ORD

- In the context of Research FUNDING
  - Open access requirements do not imply an obligation to publish results. The decision to publish is enterely up to the grant beneficiaries.
  - Open Access does not affect the decision to exploit research results commercially, e.g. patenting.
  - The decision on whether to publish through open access must come after the more general decisión on whether to publish directly or to first seek protection

From: European Help Desk factsheet “Publishing vs. patenting”

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Creative Common Licenses

Creative Commons
This symbol shows that the document, course, image, music, or art has a creative commons license.

BY
This license lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation. This is the most accommodating of licenses offered. Recommended for maximum dissemination and use of licensed materials

SA
If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

ND
This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to you.

NC
The work may not be used for commercial purposes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Licensing H2020

...as far as possible, projects must then take measures to enable for third parties to access, mine, exploit, reproduce and disseminate (free of charge for any user) this research data. One straightforward and effective way of doing this is to attach Creative Commons Licence (CC-BY or CC0 tool) to the data deposited.

Pilot on Open Research Data in Horizon 2020

Data should be covered by a CC BY license or a less restrictive license

PLoS Open Data Policy

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

HOW CAN WE START?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

- Which datasets my entity will collect or process in ATELIER?
- What my entity wants to do with those datasets?
- Are we handling personal data?
- Are we working with volunteers?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

References

- Open Acess & Data Management Online Manual

https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm

- Guidelines on FAIR Data Management in H2020

https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

- Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020

https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

- GDPR (Regulation (EU) 2016/679)

https://eur-lex.europa.eu/eli/reg/2016/679/oj

- Guidelines on Data Protection Impact Assessment

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

Contact

Cristina Martín Andonegui

cristina.andonegui@deusto.es

UNIVERSITY of DEUSTO

www.smartcity-atelier.eu

@AtelierH2020

AtelierH2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.864374

D1.3 Annex 2

The phases and steps that DPIA of Spectra will include

AmsTErdam BiLbao cItizen drivEn smaRt cities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Step #	Phase
1,1	Inspector
1,2	Inspector
1,3	Inspector
1,4	Inspector
2,1	Policy
2,2	Policy
2,3	Policy
3.1	Planner
3.1.1	Planner
3.1.2	Planner
3.1.3	Planner
3.1.4	Planner
3.1.5	Planner
3.1.6	Planner
3.1.7	Planner
3,2	Planner
3.2.1	Planner
3.2.2	Planner
3.2.3	Planner
3.2.4-3.2.8	Planner
3,3	Planner
3,4	Planner
3.4.1	Planner
3.4.2	Planner
3.4.3	Planner
3.4.4	Planner
3,5	Planner
3.5.1	Planner
3.5.2	Planner
3.5.3	Planner
3.5.4	Planner
3.5.5	Planner
3.5.6	Planner
3.5.7	Planner
3,6	Planner
3.6.1	Planner
3.6.2	Planner
3.6.3	Planner
3.6.4	Planner
3.6.5	Planner
3.6.6	Planner
3,7	Planner
3.7.1	Planner
3.7.2	Planner
3.7.3	Planner
3,8	Planner
3.8.1	Planner
3.8.2	Planner
3,9	Planner

3.9.1 Planner
3.9.2 Planner
3.9.3 Planner
3.9.4 Planner
3.9.5 Planner
3.9.6 Planner
3.10 Planner
3.10.1 Planner
3.10.2 Planner
3.10.3 Planner
3.10.4 Planner
3.10.5 Planner
3.10.6 Planner
3.11 Planner
3.11.1 Planner
3.11.2 Planner
3.12 Planner
3.12.1 Planner
3.12.2 Planner
3.12.3 Planner
3.13 Planner
4.0 Controller

Step

Company Research
Applicable legislation and regulations
Processing activities
Privacy Scan
Privacy Mission Statement
Privacy Rules of Conduct
Initial Planning
Management Structure
Assign responsibility for the protection of personal data to an internal employee
Involve senior management in the protection of personal data
Designate a data protection officer (DPO)
Assign responsibility for privacy activities within the organisation
Maintain roles and responsibility for employees involved in the protection of personal data
Report on the status of personal data protection
Perform a business risk assesment with respect to protection and management of personal data
Record of Processing Activities
Maintain record of Processing activities
Ensure identification of high-risk operations in new and existing data processings
Maintain a register of transfer mechanisms for data flows tot non-EEA countries
Identify and use other grounds for non-EU datastreams
Maintain a training and awareness programme
Maintain privacy policies
Maintain privacy policies
Document the legal basis for processing of personal data
Maintain procedures for processing special categories of personal data
Maintain procedures for processing childeren's personal data
Embed the privacy policy in daily operations
Maintain policies and procedures for ensuring continued data quality
Maintain policies and procedures for the use of automated decision making, including profiling
Maintain policies and procedures for secundary use of privacy data
Maintain policies and procedures for storing personal data
Maintain policies and procedures for the use of personal data for research purposes
Maintain policies and procedures for de-identifying of personal data
Maintain policies and procedures for obtaining valid consent
Information Risk Management
Integrate personal data protection in the general security risk assesment
Integrate personal data protection in the information security policy
Maintain technical and organisational security measures
Support the pseudonymisation and encryption of personal data
Integrate personal data protection in the business continuity planning
Regularly test the status of personal data protection
Processor risk management
Maintain requirements processors must meet in protecting (transferred) personal data
Maintain policies and procedures for engaging in and carrying out agreements with processors
Carry out due dilligence concerning personal data protection at (potential) processors
Maintain privacy notifications
Maintain notification on protection and handeling of personal data
Provide information on protection and handeling of personal data
Request and complaint handling management

Maintain policies and procedures on reacting to request for access to personal data
Maintain policies and procedures on reacting to request for information
Maintain policies and procedures on reacting to request for rectification
Maintain policies and procedures on reacting to request for discontinuation or restriction of or objections to p
Maintain policies and procedures on reacting to request for data portability
Maintain policies and procedures on reacting to request for erasure of data ('right to be forgotten')
Monitor new processing practices
Integrate personal data protection in system and product development
Maintain DPIA guidelines and templates
Carry out DPIA's for (new) programms, systems and processes
Carry out DPIA's for changes to (existing) programs, systems and processes
Involve data subjects and their representatives in carrying out DPIA's
Publish the DPIA analysis and results and consult the supervisory authority in case of residual risk
Maintaining a data breach management programme
Maintain data breach procedures for personal data breaches
Maintain a register for recording personal data breaches
Monitor existing processing practices
Carry out self-assesements on personal data protection
Maintain means of proof on GDPR compliance and/or accountability
Maintain certificates and accreditations for comfirmation of GDPR compliance
Monitor privacy developments

rocessing of personal data

D1.3 Annex 3

Draft of ATELIER Consent Form

AmsTErdam BiLbao cItizen drivEn smaRt cities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Draft of Consent Form for Volunteers

UNIVERSITY of DEUSTO

4th APRIL 2020

AmsTErdam BiLbao cItizen drivEn smaRt cities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

ATELIER: AMSTERDAM BILBAO citizen driven smart cities. Grant Agreement No: 864374. H2020 project, funded by the EU

ATELIER INFORMATION SHEET

The context of ATELIER

ATELIER is a smart city project that demonstrates Positive Energy Districts (PEDs) within 8 European cities with sustainability and carbon neutrality as guiding ambitions. Amsterdam and Bilbao are the Lighthouse cities that will generate an energy surplus of 1340 MWh of primary energy, prevent 1,7 kt of CO2- and 23 t of NOx-emissions, and invest 156 mln Euros to realise their PEDs. Together with district users, ATELIER will showcase innovative solutions that integrate buildings with smart mobility and energy technologies to create a surplus of energy and balance the local energy system. Bratislava, Budapest, Copenhagen, Krakow, Matosinhos, and Riga are the Fellow cities that will replicate and adapt successful solutions.

All cities will establish a local PED Innovation Atelier to co-produce locally embedded, smart urban solutions. In the ateliers, the local innovation ecosystem (authorities, industries, knowledge institutes, citizens) is strengthened, enhancing embeddedness and removing any obstacles (legal, financial, social, etc.) for implementation of the smart solutions. The Innovation Ateliers are designed to be self-sustaining and to live on after the project has ended. The ateliers are engines for upscaling solutions within the ATELIER-cities and replication to other EU-cities. ATELIER integrates a high degree of citizen engagement throughout the project, by actively involving local residents (>9000), local initiatives, and energy communities in activities to align technical solutions with citizens' objectives and behaviour. Each of the cities will develop a City Vision 2050 that creates the roadmap for upscaling the solutions in the long term.

ATELIER has the ambition to pave the way for "energy positive cities" in Europe. All ATELIER activities will be monitored (socially and technically), and lessons learned are systematically drawn and disseminated to relevant SET-plan groups, city networks, and innovation forums.

Purpose of the ACTIVITY

ATELIER is being run in collaboration with citizen who will lead the way for the energetic transition. In this sense, ATELIER has organized *XXXXXXXXXX* in which citizen/stakeholders are invited to participate by *XXXXXXXXXX*.

DESCRIPTION OF THE ACTIVITY

DESCRIPTION OF THE DATA THAT WILL BE RETRIEVE

JUSTIFICATION: WHY WE NEED THESE DATA?, WHAT IT IS GOING TO BE USED FOR?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Participation Form for Volunteers

1. Volunteer's Information

Full name	
Contact details (email, telephone)	

2. Contact Person Details

Full name	
Entity/Organization	
Contact Details	

3. City and/or demonstration area

Country	
City	
Neighbourhood	
PED	

4. Volunteer Questionnaire

I have read the ATELIER information sheet that provides enough details about the project (purpose, expected duration and procedures of the study)	**Yes**	**No**
I have read the ATELIER information sheet that provides enough detail of the activity and about the data that will be retrieve	**Yes**	**No**
I was informed about my right to refuse to participate or to leave the activity at any moment without any justification	**Yes**	**No**
I was notified of the contact person, in the case I have questions or doubts during the activity.	**Yes**	**No**
I was given a copy of my filled in consent form.	**Yes**	**No**
I had enough time to decide on my participation in the study.	**Yes**	**No**
I was informed about the questionnaire that I will be asked to complete	**Yes**	**No**
I was informed about the storage procedures of the study data.	**Yes**	**No**
I was assured about the confidentiality of my personal data. Publication of study results does not disclose personal data. Always according to the principles of confidentiality, I allow experts involved in the study and	**Yes**	**No**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

signing respective NDAs can utilize the information for the purpose of the study and only for this.		
ADD As many lines as necessary....		
I agree to participate in the study	**Yes**	**No**

Date: _____ Signature: _____

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

D1.3 Annex 4

Templates of Data Processor Agreements at the City of Copenhagen

AmsTErdam BiLbao cItizen drivEn smaRt cities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864374.

Changelog

CHANGE	VERSION
1.1.	Clauses 9.2. and 10.4., *(Corrected cross-references).*

UDKAST

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

[NAME]
CVR [CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the data controller)

and

[NAME]
CVR [CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

3. In the context of the provision of [NAME OF SERVICE], the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

   [NOTE: THE PARTIES SHOULD FORESEE AND CONSIDER CONSEQUENCES WHICH MAY ARISE FROM ANY POTENTIALLY UNLAWFUL INSTRUCTIONS GIVEN BY THE DATA CONTROLLER AND REGULATE THIS IN AN AGREEMENT BETWEEN THE PARTIES.]

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, 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 data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure 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. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior [CHOICE 1] specific written authorisation] / [CHOICE 2] general written authorisation of the data controller.

3. [OPTION 1 SPECIFIC PRIOR AUTHORISATION] The data processor shall engage sub-processors solely with the specific prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data controller can be found in Appendix B.

   [OPTION 2 GENERAL WRITTEN AUTHORISATION] The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract

or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, [PLEASE INDICATE THE COMPETENT SA], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, [PLEASE INDICATE THE COMPETENT SA], prior to processing where

a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within [NUMBER OF HOURS] after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation [OPTION 1] to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so / [OPTION 2] to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

2. [OPTIONAL] The following EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services:

    a. […]

The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

   On behalf of the data controller

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

On behalf of the data processor

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Appendix A Information about the processing

[NOTE: IN CASE OF SEVERAL PROCESSING ACTIVITIES, THESE ELEMENTS MUST BE COMPLETED FOR EACH OF THE PROCESSING ACTIVITIES.]

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

[DESCRIBE THE PURPOSE OF THE PROCESSING].

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

[DESCRIBE THE NATURE OF THE PROCESSING].

A.3. The processing includes the following types of personal data about data subjects:

[DESCRIBE THE TYPE OF PERSONAL DATA BEING PROCESSED].

[FOR EXAMPLE]

"Name, e-mail address, telephone number, address, national identification number, payment details, membership number, type of membership, attendance at fitness centre and registration for specific fitness classes."

[NOTE: DESCRIPTION SHOULD BE MADE IN THE MOST DETAILED POSSIBLE MANNER AND, IN ANY CIRCUMSTANCE, THE TYPES OF PERSONAL DATA MUST BE SPECIFIED FURTHER THAN MERELY "PERSONAL DATA AS DEFINED IN ARTICLE 4(1) GDPR" OR STATING WHICH CATEGORY ("ARTICLE 6, 9 OG 10 GDPR") OF PERSONAL DATA IS SUBJECT TO PROCESSING.]

A.4. Processing includes the following categories of data subject:

[DESCRIBE CATEGORY OF DATA SUBJECT].

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

[DESCRIBE THE DURATION OF THE PROCESSING].

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

[OPTIONAL] [IF APPLICABLE, DESCRIBE THE TIME PERIODS OF PRIOR NOTICE FOR AUTHORISATION OF SUB-PROCESSORS]

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

[DESCRIBE THE PROCESSING THAT THE DATA PROCESSOR HAS BEEN INSTRUCTED TO PERFORM].

C.2. Security of processing

The level of security shall take into account:

[TAKING INTO ACCOUNT THE NATURE, SCOPE, CONTEXT AND PURPOSES OF THE PROCESSING ACTIVITY AS WELL AS THE RISK FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS, DESCRIBE ELEMENTS THAT ARE ESSENTIAL TO THE LEVEL OF SECURITY]

[FOR EXAMPLE]

"That the processing involves a large volume of personal data which are subject to Article 9 GDPR on 'special categories of personal data' which is why a 'high' level of security should be established."

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

[DESCRIBE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE REQUIREMENTS FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES]

[DESCRIBE REQUIREMENTS FOR THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT]

[DESCRIBE REQUIREMENTS FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING]

[DESCRIBE REQUIREMENTS FOR ACCESS TO DATA ONLINE]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING STORAGE]

[DESCRIBE REQUIREMENTS FOR PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED]

[DESCRIBE REQUIREMENTS FOR THE USE OF HOME/REMOTE WORKING]

[DESCRIBE REQUIREMENTS FOR LOGGING]

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

[DESCRIBE THE SCOPE AND THE EXTENT OF THE ASSISTANCE TO BE PROVIDED BY THE DATA PROCESSOR]

[DESCRIBE THE SPECIFIC TECHNICAL AND ORGANISATIONAL MEASURES TO BE TAKEN BY THE DATA PROCESSOR TO PROVIDE ASSISTANCE TO THE DATA CONTROLLER]

C.4. Storage period/erasure procedures

[STATE STORAGE PERIOD/ERASURE PROCEDURES FOR THE DATA PROCESSOR, IF APPLICABLE]

[FOR EXAMPLE]

"Personal data is stored for [STATE TIME PERIOD OR INCIDENT] after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses."

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

[STATE WHERE PROCESSING TAKES PLACE] [STATE THE DATA PROCESSOR OR SUB-PROCESSOR USING THE ADDRESS]

C.6. Instruction on the transfer of personal data to third countries

[DESCRIBE AN INSTRUCTION ON THE TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY OR INTERNATIONAL ORGANISATION]

[STATE THE LEGAL BASIS FOR TRANSFER PURSUANT TO CHAPTER V GDPR]

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

[DESCRIBE PROCEDURES FOR THE DATA CONTROLLER'S AUDITS, INCLUDING INSPECTIONS, OF THE PROCESSING OF PERSONAL DATA BY THE DATA PROCESSOR]

For example:

"The data processor shall [STATE TIME PERIOD] at [THE DATA PROCESSOR'S/THE DATA CONTROLLER'S] expense obtain an [AUDITOR'S REPORT/INSPECTION REPORT] from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of [AUDITOR'S REPORT/INSPECTION REPORT] may be used in compliance with the Clauses:

[INSERT 'APPROVED' AUDITOR'S REPORTS/INSPECTION REPORTS]

The [AUDITOR'S REPORT/INSPECTION REPORT] shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required."

[OR]

"The data controller or the data controller's representative shall [STATE TIME PERIOD] perform a physical inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data controller may perform an inspection of the data processor when the data controller deems it required"

[AND, IF APPLICABLE]

"The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection."

C.8. [IF APPLICABLE] Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

[IF APPLICABLE, DESCRIBE PROCEDURES FOR THE DATA CONTROLLER'S AUDITS, INCLUDING INSPECTIONS, OF PROCESSING OF PERSONAL DATA BY THE SUB-PROCESSOR]

[FOR EXAMPLE]

"The data processor shall [STATE TIME PERIOD] at [THE DATA PROCESSOR'S/THE DATA CONTROLLER'S] expense obtain an [AUDITOR'S REPORT/INSPECTION REPORT] from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of [AUDITOR'S REPORT/INSPECTION REPORT] may be used in compliance with the Clauses:

[INSERT 'APPROVED' AUDITOR'S REPORTS/INSPECTION REPORTS]

The [AUDITOR'S REPORT/INSPECTION REPORT] shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor or the data processor's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology."

[OR]

"The data processor or the data processor's representative shall [STATE TIME PERIOD] perform a physical inspection of the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing to ascertain the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data processor may perform an inspection of the sub-processor when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

Based on the results of such an inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses."

[AND, IF APPLICABLE]

"The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses."

[AND, IF APPLICABLE]

"The data processor's and the sub-processor's costs related to physical supervision/inspection at the sub-processor's facilities shall not concern the data controller – irrespective of whether the data controller has initiated and participated in such inspection."

Appendix D The parties' terms of agreement on other subjects