Data Management Plan

Leading partner	CES
Type	Report
Dissemination level	PU - Public
Work package	WP1
Deliverable	D1.3
Due date	November 2018
Version	1.0

Project	Healthy corridor as drivers of social housing neighbourhoods for the co-creation of social, environmental and marketable NBS
Acronym	URBiNAT - Urban inclusive and innovative nature
	This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 776783

List of Authors and Reviewers

Authors	**Reviewers**
Nathalie Nunes - CES	Gonçalo Canto Moniz - CES
Sandra Silva Carvalho - CES	Matthieu Roest - IKED
Sheila Holz - CES	Rita Pais - CES
Contributors	
CF - Laura Ohler	
CES - Gonçalo Canto Moniz	
CIBIO - José Miguel Lameiras and Beatriz Truta	
DTI - Marie Nicole Sorivelle and Knud-Erik Hilding-Hamann	
IKED - Thomas Andersson	
ITEMS - Sébastien Levy and Tom Mackenzie	
IULM - Guido Ferilli	
UNG - Marco Acri	

Document history

Date	**Version**	**Author**	**Summary of change**
26 Oct. 2018	0.1	Nathalie Nunes Sandra Silva Carvalho Sheila Holz	First draft
28 Nov. 2018	1.0	Nathalie Nunes Sandra Silva Carvalho Sheila Holz	Data management plan Initial version

Fonts

Montserrat	by Julieta Ulanovsky
Source Sans Pro	by Paul D. Hunt

List of acronyms

Acronym	Description
AGA	Annotated Model Grant Agreement
API	Application Programming Interface
CAD	Computer-Aided Design
CIPA	Classified Information Protection Act
CNIL	Commission Nationale de l'Informatique et des Libertés (French data protection authority)
CNPD	Comissão Nacional de Proteção de Dados (Portuguese data protection authority)
CoP	Community of Practice
DMP	Data Management Plan
EC	European Commission
EU	European Union
FAIR	Findable, Accessible, Interoperable, Re-usable (data)
GBA	Gegevensbeschermingsautoriteit (Belgian data protection authority)
GA	Grant Agreement
GDPR	General Data Protection Regulation
GIS	Geographic Information System
HC	Healthy Corridor
IPR	Intellectual Property Rights
NBS	Nature-Based Solution
ORDP	Open Research Data Pilot
SC	Steering Committee
SME	Small and Medium-sized Enterprise
WP	Work package

Introduction

The purpose of this document is to provide an initial version of URBiNAT's Data Management Plan (DMP), which as a living document will be updated during project development when the need arises in order to improve the internal processes. The DMP derives from Task 1.3 "Innovation, IPR and data management" of Work Package 1 "Management of consortium and project's general implementation". It constitutes the Deliverable D1.3.

This plan, delivered by the Steering Committee, reveals the expected data to be generated, whose analysis will generate outputs and will be made accessible, on the basis of raw and curated data. It addresses how data will be collected (including from third parties), quality controlled, stored, protected, shared and preserved, during and after the end of the project's implementation. URBiNAT's DMP mainly addresses the issues of the DMP template provided by the European Commission (EC) for projects funded under Horizon 2020, which were answered based on the consultation to all Work Package Leaders, as well as members of the Steering Committee.

URBiNAT's ambitious approach of setting up a variety of Nature-Based Solutions (NBS) in different cities and spanning different use cases will inherently lead to the generation of data, which may go beyond the qualification of 'research data'. It is important to ensure that all data are well managed during the project's lifetime and beyond, and preserved for further use. The plan ensures that all data are collected and annotated in the required format for easy access, usability and reliability, and guarantees the privacy of all parties, participants and stakeholders.

All partners in the URBiNAT project will work in compliance with EU General Data Protection Regulation (GDPR). Observers and partners involved in non-EU countries (Brazil, Iran, Oman, China and Japan), will also explicitly assume their agreement to the data protection safeguards required by EU regulation, as contemplated in this DMP, the Grant Agreement (GA) and the Consortium Agreement.

Therefore, apart from making data and data control central in the design of its solutions, the project will install appropriate data management principles. URBiNAT's ethics principles and guidelines will be applied to its DMP and, consequently, to data collection and management throughout the project.

1. Data summary

Questions to be addressed:
1.1 What is the purpose of the data collection/generation and its relation to the objectives of the WP?
1.2 What types and formats of data will the WP collect/generate?
1.3 Will you re-use any existing data and how?
1.4 What is the origin of the data?
1.5 What is the expected size of the data?
1.6 To whom might it be useful ('data utility')?

The following table presents the tasks where data will be collected/generated throughout the project's implementation:

Work Packages and Tasks		Partner Leader
WP 1 - Management of consortium and project's overall general implementation		CES
T1.1	Coordinate and monitor the implementation of activities	CES
T1.2	Scientific coordination	CES
T1.3	Innovation, IPR and data management	CES
T1.4	Ethics analysis	CES
T1.5	Inclusion of cross cutting dimensions: human rights and gender, international cooperation	CES
T1.6	Administrative and financial coordination	CES
T1.7	Communication with EC, among partners and day-to-day point of contact	CES
WP2 - Living labs in frontrunner and follower cities		ICETA
T2.1	Local diagnostics in Frontrunner and Follower	IULM
T2.2	Networking	CIBIO/UNG
T2.3	Coaching and Sharing to create the CoP	IKED
T2.4	Local Urban Plans for URBiNAT cities	CES
T2.5	Common Road Map for NBS	CIBIO/ UNG
WP3 - Citizen engagement in support of NBS		DTI
T3.1	Stocktaking and research on participatory culture	DTI
T3.2	Design of community-driven process	CES
T3.3	Content for digital communication support	IKED
T3.4	Application and sharpening of digital communication support	IKED
T3.5	Participatory training workshops	GUDA
WP4 - Healthy corridors and URBiNAT's NBS catalogue		CES
T4.2	Territorial and technological NBS Co-design	IAAC
T4.3	Manufacturing of technological NBS prototypes for testing and demonstration	DTI

T4.4	Healthy Corridor concept. Urban co-planning methodology for territorial and technological NBS	CES
T4.5	Models, diagrams and technical drawings to characterize/define urban planning	CES
T4.6	Co-implementation in front-runner cities of the Healthy Corridor	CES
T4.7	Healthy Corridor market potential for Social and Solidarity Economy	CES
WP5 - Observatory for Urban Inclusive and Innovative Nature - OURBiNAT		IULM
T5.1	Data management	IULM
T5.2	Monitoring and evaluation and simulation	IULM
T5.3	Health effects and impact on well-being of NBS	OWL
T5.4	Economic and social impact of NBS	UA
T5.6	Action research and systematization for the development of an EU-wide reference framework for NBS	CES
WP6 - Dissemination and Communication		ITEMS
T6.1	Develop and implement a communication and dissemination plan	ITEMS
T6.2	Development of materials and tools	CES
T6.3	Dissemination of publications and the NBS catalogue	ITEMS
T6.4	Networking and participation in events and conferences	ITEMS
WP7 - Market Assessment and Business Case Development for NBS		CF
T7.1	Select best practice NBS projects within the 3 front-runner cities based on their market potential	CF
T7.2	Conduct interviews with local stakeholders	CF
T7.3	Write up of business cases for the most marketable and bankable NBS	CF
T7.4	Select business cases for replication and scaling	CF

1.1. Purpose of data collection/generation and its relation to the project's objectives

URBiNAT will collect/generate data in order to achieve its objectives, namely:

- ❑ Promote social cohesion through the activation of Living Labs and an inclusive community of practice.
- ❑ Achieve new models of urban development addressing NBS for inclusive urban regeneration through an innovative public space: Healthy Corridors.
- ❑ Create value around urban, inclusive and innovative nature through widespread knowledge sharing and replicability, as well as the monitoring, dissemination and market replication of knowledge produced and demonstrated.

In **WP2** (Living labs in front-runner and follower cities) data will be collected/generated**,** mainly in Task 2.1 (local diagnostics in front-runner and follower cities) to describe the local conditions of the deprived areas, to determine a baseline for social, environmental and economic challenges,

but also to understand local needs and expectations. It will include the mapping of the deprived areas, production of behavioural mapping, identification of community assets and urban capital. Data collection will support the design of the Healthy Corridors. This task will be developed in two stages:

- ❏ Stage 1 - collection of existing data: GIS, CAD, and statistical databases; spatial, social and economic reports/data; previous experience in participatory processes; previous experiences in NBS design and implementation.
- ❏ Stage 2 - collection of new data: Includes territorial, social and economic data, namely identifying local needs and expectations, behavioural mapping, as well as the survey of indicators on participatory planning and governance, social justice and social cohesion, public health and well being, economic opportunities and green jobs.

This task will also collect/generate data on participatory processes and practices, social and solidarity economy (policies and practices), and existing NBS in each city to adopt new NBS and social processes articulated with the existing ones and their context. During Stage 1, the cities are asked about their detailed experience, including a self evaluation of the events/processes applied so far, but also local expectation and future initiatives.

Apart from T2.1, which will collect the largest volume of data, T2.2, T2.3, T2.4 and T2.5 will also collect/generate data:

- ❏ Networking (task 2.2), will be based on Task 2.1 and will focus on the development of local networks of citizens and stakeholders. It will include the establishment of local collaborative platforms and the implementation of Workshops and meetings from which new data will be developed.
- ❏ Coaching and Sharing (task 2.3) will establish a Community of Practice in order to boost cooperation between cities implementing NBS. For this cross-pollination data will be collected and generated to be disseminated.
- ❏ Local Urban Plans (task 2.4) for URBiNAT cities. This task will generate the planning, design and construction plans that will be delivered to each city and could later be replicated as a URBiNAT product. Data generated from this task will be produced in articulation with WP4.
- ❏ Common Road Map for NBS (task 2.5). This task will compile data and reflect on the experience from the previous tasks.

WP3 (Citizen engagement in support of NBS), data will be collected to better understand current participatory processes and digital platforms used to engage citizens and relevant stakeholders in the co-creation process. By opening up research and innovation processes to the public, the WP3 team can better assess the values, needs and expectations of these individuals and organisations.

- ❏ In knowing what was done before, what worked, and what did not work will aid in the developing of opportunities to further engage, strengthen and increase the implementation of participatory processes and digital communication platforms across cities, diverse target groups and key stakeholders, project facilitators and operators taking part in task activities such as surveys, workshop training activities, etc.
- ❏ The implementation of new participatory processes and experiments will generate new and additional data to be collated for refining of participatory process guidance, training and amplification.
- ❏ The participatory process training workshops will produce data to be collected on the relevance and impact of these workshops for the participants and participatory processes they will conduct in the future.

In **WP4** (Healthy corridors and URBiNAT's NBS catalogue), data is related to the development of the NBS catalogue and design of Healthy Corridors (HC). Data collection will characterize the area of implementation of the HC in terms of environmental, social and economics indicators. The diagnostic will support co-design decisions offering a portrait of the area and will provide data to customize the NBS, in order to understand their capacity of adaptation to each city.

- ❏ The revisions of the NBS catalogue and the development of the territorial and technological solutions will generate new data related to the technical specifications of the NBS.
- ❏ The development of the Healthy Corridor strategy and urban projects will generate a design process, with physical drawings and models, and with digital drawings (dwg), digital models, digital photos, project description (doc).
- ❏ The implementation of the HC will generate technical drawing and documents to support the construction site.

WP5 (Observatory for Urban Inclusive and Innovative Nature - OURBiNAT) will use data collected in the local diagnostics of WP2 to monitor and evaluate the local context. This coordination and transfer of data also concerns WP3, WP4 and WP6. The tasks of the WP5 will perform the maintenance and development of the data, as well as their use in support of the front-runner and follower cities. A specific focus on the NBS in terms of well-being, social and economic effects, and local governance will be dedicated through the tasks 5.3, 5.4 and 5.5. During task 5.6, the action-research, additional quantitative and qualitative data will be collected/generated in order to systematize the project's trajectory and support the establishment of a EU-wide reference framework for NBS.

Data collection/generation in **WP6** (Dissemination and communication), will include the building of an extensive contact list of stakeholders interested (or potentially interested) in receiving updates on the project and its progress. Dissemination activities will also generate data during meetings, participation in workshops, website, newsletters and other dissemination actions and materials.

In **WP7** data will be collected for the purpose of market assessment and business case development for NBS. One of the main objectives of WP7 is to create value on URBiNAT's NBS based products for businesses in all intervention cities. In order to meet this objective, best-practice NBS projects and their underlying business cases must be identified. This includes a clarification of the definition of NBS and how they are to be measured and managed by either new start-up businesses or already established organisations in the area. Aspects of value-creation through social innovation in the NBS business model will be considered as well. Further, data and information will incorporate aspects that help document and cast light on the role of policy-related factors in either supporting or impeding innovation.

- ❏ Throughout the process of identifying best-practice business cases, one-on-one in-depth interviews will be conducted with people who played a role in either developing or helping to underpin energy-efficient, green, and sustainable business models. Key stakeholders in this respect encompass urban planners, local municipalities, citizens, start-ups, NBS experts, and all kinds of businesses.
- ❏ As a result of this process, best-practice cases will be selected for further scaling and diffusion.
- ❏ Based on the resulting data and insights, analysis will be undertaken on the lessons for policy and help structure a portfolio of recommendations for measures applicable under diverse circumstances in support of best practice.

1.2. Types and formats of collected/generated data

WP2 will use the existing CAD, GIS, statistical databases and collect new data through fieldwork. Existing and surveyed data will be used to produce technical reports - the local diagnostics.

WP3 will gather personal, social and economic data using various tools (including digital) and methods during surveys, participatory training workshops, digital communication support actions and relayed in reports, project presentations, and a participatory handbook for NBS. Data will be generated in the Word, PPT, Excel and PDF formats. Furthermore, some data will be treated as statistical data in a form that can be read by statistical programs like SPSS.

WP4 will generate data related to the impact of the NBS in the social (related to the profiles of the communities and the ways in which the communities use the area), economic (related to the activities produced by the citizens and to the economic profile of the citizens) and environmental context (related to the quality of the water, air and soil); and also urban plan data (related to former urban plans, architecture projects, landscape project) and iconography (drawings, photographs, models, videos, posters, publications). The transformations observed in the territory will produce/generate quantitative and qualitative data. These data will have different formats - word, excel, pdf, png, jpg, dwg, audio and video - mp3 / mp4 / mov.

WP5 will process all types and formats of data collected/generated by the others WPs. The goal of the WP5 is to use and process all formats that will converge in the monitoring, evaluation and simulation of the local contexts in an interdisciplinary approach. Ad-hoc formats, like .nna, .var, .wtx and .hid will be generated for the specific use of Artificial Neural Network computational tools.

WP6 will collect contact details (e.g. e-mails, phone, social networks, identification data) of partners, participants and any person interested in the project and its progress, in accordance with GDPR requirements. Word/Excel files will be produced with this information.

WP7 will generate qualitative analysis in Word files, including audio recordings, transcriptions, and notes from the interviewer. Initially, desktop research will be conducted to analyse the market of the front-runner and follower cities. In this process word files will be used to gather all necessary information (see local diagnostic document). During the market survey, local community members will be invited in an open workshop that will generate ideas for NBS, local supply demands, and existing biotechnological solutions. The findings from these workshops will be documented in Word and audio files. In an online survey, NBS will be rated according to their popularity among citizens. Participation in this activity will be anonymised. The results will be presented in a comparative statistic that lists the winners of the rating. This data will be archived with a software that has not been determined yet. Key stakeholders (start-ups, citizens, city administration, corporate clients, NBS experts, researchers and technical experts) will be interviewed in a multi-stakeholders analysis. The in-depth one-to-one interviews are used to calculate the costs, benefits, roles and responsibilities of each NBS project delivery. These interviews will be stored as anonymised transcriptions and audio files. The participants will also have to sign a consent form. In the end of the empirical research, business cases for the most marketable NBS will be scaled and replicated. This information will be handled as open-source within the URBiNAT project and stored in a Word file. Policy recommendations for replication and scaling the best-practice NBS business cases will be shared with all follower and front-runner cities involved in the process in a PDF document.

1.3. Reuse of existing data

In the scope of **WP1**, information on the project, contact details and partner information will be shared with relevant internal and external interlocutors, through internal and external communication tools, such as Basecamp, the project's website and the newsletters.

Concerning **WP2**, the analysis of existing data will be conducted in the first stage of the local diagnostic's data collection, which is based mainly on the reuse of existing data collected at regional and local level, including statistical data, assessment of existing reports and specific studies accredited by the local authorities. The data collected in the local diagnostic in its second stage, namely at local level, may determine reuse of additional data not included in stage 1, as well as existing info/data stored at NGOs or private archives. The data collected in this WP may be either open to the public or protected, according to the origin and subject: more precise information on this will be given in a DMP update.

WP3 has two stages of data reuse. The first one aims to build on existing knowledge and data collected during the initial desk research and will assist in understanding what was and/or what is being done in the cities from a participatory and digital communication perspective. These due diligence activities will provide a bedrock of existing knowledge that may confirm, complement or contradict the validity and relevance of initial conclusions on participatory practices or digital platforms. The second stage aims to provide context. Data collected from the initial desk research will assist in the formulating of survey questions to pose to target groups in order to provide contextual clarity, trends and other interesting insights stemming from the survey results.

WP4 will reuse data already produced by the NBS partners, in the context of other projects. Best practices already implemented will act as references for the NBS and HC development.

The data collected in different phases of the project's implementation will be used, in the scope of **WP5**, for comparing the implementation of the activities/NBS. Most of the data will be secondary, namely in the first stage of the task 2.1 (Local diagnostics). The second stage will add new data.

During the development of **WP6**, the URBiNAT contact list will be enlarged based on the consent and reuse of existing contact lists from project's partners. Additional contacts may come from the implemented social networks account referring to the website and individuals of the partnership.

The activities developed under **WP7** will not reuse data since they will be based on exploratory research.

1.4. Data origin

Data originated in all the project's Work Packages derive from many, varied sources.

A formal permission will be asked to the institutions that provide non-public data to the project, namely municipalities and private/public archives.

For **WP1**, data originates from reports, project findings and results, research production, contact details of partners and database of external contacts for communication and dissemination.

In **WP2**, data originates mainly from the municipalities and local partners. It will also be collected from the National and European Observatories, as well as from online geographic databases (Google Earth, Bing Maps, Apple maps).

In **WP3**, data will also be collected mainly from the municipalities and local partners. Additional sources include data from: desk research, surveys and one-on-one dialogue with citizens, activity-related meetings, workshops and other participatory experiences in cities covering non-NBS solutions to gain good practice insight from these experiences. It will also use relevant results from WPs 2, 4 and 7.

In **WP4**, the data is collected in two stages. The first stage uses the data collect in the Local Diagnostic (WP2) from the municipalities GIS platform, surveys, reports, as well as from the statistical institutions. The second stage will collect quantitative and qualitative data from the workshop activities (handout, video recordings, questionnaires) promoted by WP3 to co-design the NBS solutions and the HC urban plan.

WP5 development is divided in two stages. In the first stage the data are originated by the task 2.1 of the project. For this data, primary and secondary, there will be analysis and evaluations from the tasks of the WP. The first stage will use the data already existing from each city. In the second stage, that occurs during the development of the project, the data will be collected from the cities and the partner involved in various aspect of the urban environment and life, and compared with the existing information.

In **WP6**, the data originates from: information provided by the partners regarding the development of their activities, social media actions and number of visits to the URBiNAT website.

In **WP7**, the data originates from one-on-one in-depth interviews.

1.5. Size of data

The data originated in URBiNAT derives from many sources and will be provided in various formats. This includes standard resolution for Word documents, Excel spreadsheets and digital documents for communication and dissemination, and also high-resolution images, videos, economic data, social data, and other data, to support the WPs' activities. In this sense, the exact size of the data is unknown at this stage but it is anticipated to reach several Terabytes - perhaps 1 Petabyte (1000 Terabytes).

1.6. Data utility

The data collected and generated during the project will be used for internal and external purposes. Internal use relates to project management. For instance, to feed into URBiNAT's governing and advisory bodies, consortium partners, cities and internal stakeholders. Data collected and generated will also feed into the tasks and activities of all Work Packages (WP2, WP3, WP4, WP5, WP6, WP7), some specific partners activities, such as NBS developers partners (IAAC, CIBIO, and CES) and by partners leading communication and dissemination activities.

In addition, the data are useful for researchers, cities, public and private authorities working in the field of NBS, and for upcoming businesses (start-ups) in the intervention cities and other cities around the world interested in sustainable urban city solutions.

2. Fair data

2.1. Making data findable, including provisions for metadata

Questions to be addressed:
2.1.1 Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?
2.1.2 What named conventions do you follow?
2.1.3 Will search keywords be provided that optimize possibilities for re-use?
2.1.4 Do you provide clear version numbers?
2.1.5 What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

As suggested during the partner's meeting organized in Brussels in October 2018, URBINAT may consider to adopt Oppla to host its data.

Oppla hosts a variety of content, including NBS products and case studies, and will soon host metadata for NBS datasets too. The datasets themselves will generally be stored elsewhere online. All of this content will be findable both on the Oppla website and via the Oppla API.

The website offers a variety of tools to help find content, including text search, various filters and an interactive map. The API will feature a powerful Solr search facility, which we plan ultimately to build into the website as well. It is planned to offer a metadata structure compliant with the DCAT application profile for data portals in Europe.

Further details will be provided in future versions of this DMP.

2.2. Making data openly accessible

Questions to be addressed:
2.2.1 Which data produced and/or used in the project will be made openly available as the default? If certain datasets cannot be shared (or need to be shared under restrictions), explain why, clearly separating legal and contractual reasons from voluntary restrictions.
2.2.2 How will the data be made accessible (e.g. by deposition in a repository)?
2.2.3 What methods or software tools are needed to access the data?
2.2.4 Is documentation about the software needed to access the data included?
2.2.5 Is it possible to include the relevant software (e.g. in open source code)?
2.2.6 Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories which support open access where possible.
2.2.7 Have you explored appropriate arrangements with the identified repository?
2.2.8 If there are restrictions on use, how will access be provided?
2.2.9 Is there a need for a data access committee?

2.2.10 Are there well described conditions for access (i.e. a machine readable license)?
2.2.11 How will the identity of the person accessing the data be ascertained?

URBiNAT intends to make the data collected and produced in the life cycle "as open as possible, and as closed as necessary" following the EU Guidelines on FAIR Data Management in Horizon 2020. The project will collect, produce and manage data in all Work Packages as demonstrated above.

The access to data collected and generated can be divided into the following three categories:

i) Fully open data - openly accessible to all. For example, information on the project and its results made available on the website, and research results in open scientific publications.

ii) Conditional access - data that can be made public to all, but requires a specific action by the potential user to access such data. For example, download public deliverable upon specific registration of interest on the website.

iii) Restricted access - data requiring a higher level of protection, and for which access will be given only to specific partners involved in using this data. This includes personal data, sensitive data, data collected in the cities. Categorisation and verification will be made by the partner responsible for data collection in each Work Package during the project progress. Restricted access may also be applied to other data related to innovation, IPR and commercialisation of the project's results. As referred to under Article 29.3 of the Grant Agreement: "*As an exception, the beneficiaries do not have to ensure open access to specific parts of their research data if the achievement of the action's main objective, as described in Annex 1, would be jeopardised by making those specific parts of the research data openly accessible. In this case, the data management plan must contain the reasons for not giving access.*"

External users may access the project's public data mainly through the URBiNAT website and social media accounts. The partners, including municipalities, may also make such public data available through their websites and social media channels.

Since URBiNAT is part of the H2020 Open Research Data Pilot (ORD Pilot), research data may be also accessed through a repository.

Open access and open research data

URBiNAT firmly believes in openness to be a major factor for innovation. There are many examples of how open innovation and open source are successful models, especially in domains where many and varied stakeholders are required to bring about effective change. Openness has many facets. The most important ones for the URBiNAT consortium are, following Carlos Moedas's (European Commissioner for Research, Science and Innovation) strategy of the 3 Os, Open Science, Open Innovation and Open Data:

(i) **Open project collaboration**. All partners are committed to developing relationships with external partners for mutual benefit. Making contacts with partners of similar projects and establishing collaboration is considered beneficial to all. Open collaboration in URBiNAT is understood in a trans-disciplinary way, opening research processes to the wider public and allowing new forms of collaboration as intended in the action research stream of the project.

(ii) **Open source technology**. From a technology perspective, the project builds upon open source technologies, such as some NBS technologies and wants to share its results with actors and stakeholders both in and outside of the NBS community. Business models and exploitation strategies are not based on locking down access to project results, but on providing added value through services.

(iii) **Open access to scientific results**. From a scientific perspective, the consortium favours open access to its scientific output, which is supported by several project members' internal policies of supporting open access in general.

(iv) **Open access to research data**. URBiNAT is part of a pilot action on open access to research data and is thus committed to providing access not only to project results and processes, but also to data collected during that process. The general policy of the URBiNAT project is to apply "open by default" to its research data, with exceptions being made based on privacy, competitiveness and the relationship between researchers and cases; ethical rules on anonymity are thus highly relevant and need to be agreed with each of the case participants.

Open access strategy for publication

URBiNAT is part of the H2020 pilot action on open access to research data. In line with the EC policy initiative on open access, which refers to the practice of granting free online access to research articles, the project is committed to follow a publication strategy considering a mix of both 'Green open access' (immediate or delayed open access that is provided through self-archiving) and 'Gold open access' (immediate open access that is provided by a publisher) as far as possible.

All deliverables (reports, software, data, media, other) labelled as "*public*" will be made accessible via the URBiNAT website (http://urbinat.eu/). The publications stemming from the project work will also be made available on the website as far as it does not infringe the publishers rights as well as on the OpenAIRE platform https://www.openaire.eu/.

All outcomes of the project labelled as "*public*" will be distributed under specific free/open license, where the authors retain the authors' rights but the users can redistribute the content freely. The following are a few relevant sources for deciding on the specific license for each outcome:

- Data:
  - A definition of Open Data: http://opendefinition.org/
  - Licenses: http://opendefinition.org/licenses/

- Software:
  - Free Software
    - The definition: http://www.gnu.org/philosophy/free-sw.html
    - Licenses: http://www.gnu.org/licenses/licenses.html

  - Open Source Software
    - The definition: https://opensource.org/osd-annotated
    - Licenses: https://opensource.org/licenses

- Reports, publications, media:
  - Creative Commons
    - Explanation: https://creativecommons.org/about/
    - Licenses: https://creativecommons.org/licenses/

- ❏ Choose a license: https://creativecommons.org/choose/

Open access and open data handling process

The internal procedures to grant open access to any publication, research data or other innovation stemming from the URBiNAT project follow a lightweight structure, while respecting ethical issues at all time.

The main workflow starts at the WP level, where each team is responsible for respecting ethical procedures at all times during the data gathering and processing steps. The WP team members are also responsible for making any data anonymous, if applicable. For any publication the Steering Committee needs to be informed; agreement has to be reached within the WP for making any outcome openly available; the final approval is done by the Steering Committee.

The data collected and generated will be stored and made accessible for the specific use of specific partners on the server of URBiNAT's Observatory (OURBiNAT - WP5).

Consortium partners have access to data internally, through URBiNAT's collaborative platform (Basecamp), the main tool for sharing and collaborating on documents. All partners have access to this platform upon invitation and can contact each other and share documents through it. However, not all data will be fully accessible to all partners. For instance, financial reports will be collected and managed only by the Project Management Office.

To access data, users will need access to the internet, web browsers, and other specific softwares such as office softwares (for example, those provided by Microsoft Office, OpenOffice, LibreOffice) for documents, spreadsheets and presentations, pdf readers, GIS, CAD, Adobe creative suite. Documentation about these softwares will be included. All useful softwares can be included if they are open source and available in all partner countries.

According to each specific storage use, data and associated metadata, documentation and code will be deposited on the Basecamp platform, URBiNAT's website, the Observatory's server, and in a certified repository for open access to research data. Appropriate arrangements are under exploration with Oppla.

All content on the Oppla website will be openly accessible. The API will be protected by a system of API keys (although this may only apply to editing), but keys will be easy to obtain, and available to all legitimate consumers of the content. Access to datasets themselves will be controlled by the dataset providers, but they will be encouraged to make the data as open as possible, and to specify any restrictions in the metadata.

In other words, the datasets will be stored online on a semantic web. All the data will be findable both on the web and via API. All contents will be openly accessible. Only widely recognised open formats will be implemented to maximize interoperability. This will allow others to use from remote data and metadata. The use of widely used standards will be encouraged and controlled by the dataset providers.

Regarding restrictions on use:

- ❏ Access to Basecamp is only granted upon invitation and with credentials to use specific tools and/or administration credentials. Persons may be invited to access Basecamp as clients but, in this case, can only view some parts of the data. Public links of specific pages on Basecamp can also be shared, but do not enable access to the platform as a whole;

- ❏ Reports to the EC are made available through the Participant Portal. Only coordinator credentials can be used to submit, but partners can access and complement reports. These reports will also be made accessible to partners on the collaborative platform of the Consortium (Basecamp);
- ❏ Other reports to be shared with governing bodies and advisory boards may be shared on Basecamp in specific areas with limited access or by email linking back to Basecamp with specific notification on confidentiality and/or restricted use (avoiding printing for example);
- ❏ Public deliverables can also be shared on the website, however it is foreseen to ask for identification and justification of interest through a specific form before receiving the document by email;
- ❏ As part of a Community of Practices, cities and other relevant stakeholders will access specific data upon invitation and/or registration;
- ❏ A version of the NBS catalogue will be open access through the website;
- ❏ Healthy Corridor solutions will be part of technical reports, partly open access, namely drawings and 3D models;
- ❏ In the case of Participatory Practices, restrictions will be managed according to specificities of the different kinds of research data.

The URBiNAT project has a Steering Committee that reports to the General Assembly on cases requiring IPR protection and derogation to open access principles.

No other detailed described conditions for access (i.e. a machine-readable license) are available at this moment.

Regarding the identity of persons accessing the data, the following will be required:

- ❏ identification and justification of interest to the research manager and communication team;
- ❏ registration as a participant in the relevant participatory community. A participatory community is a group of people involved in a specific NBS development in a specific city and also the community of facilitators, moderators and key-people taking part in the Participatory training workshops undertaken in WP3.

2.3. Making data interoperable

Questions to be addressed:
2.3.1 Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?
2.3.2 What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?
2.3.3 Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability?
2.3.4 In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?

According to the discussions underway with Oppla, the API will be designed for maximum interoperability, by implementing widely used standards and offering detailed documentation. This will allow the content and metadata to be used (searched, consumed and edited) by many other websites with relative ease. The format (and hence the level of interoperability) of the

datasets themselves will be controlled by the dataset providers, but they will be encouraged to use widely recognised open formats to maximise interoperability.

This does not include personal data.

Further details will be provided in future versions of this DMP.

2.4. Increase data re-use (through clarifying licences)

Questions to be addressed:
2.4.1 How will the data be licensed to permit the widest re-use possible?
2.4.2 When will the data be made available for re-use? If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.
2.4.3 Are the data produced and/or used in the project useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why.
2.4.4 How long is it intended that the data remains re-usable?
2.4.5 Are data quality assurance processes described?

According to the discussions underway with Oppla, dataset providers will be encouraged to specify a widely used licence for each dataset in the metadata submitted to Oppla. This will clarify where the data can be reused. Clear terms of use for Oppla itself, which cover content and metadata hosted on Oppla and the API, can be found at https://oppla.eu/oppla-terms-use.

Databases produced in CAD and GIS softwares, and statistical data are usually compatible across different software solutions. They can also be converted to other file formats to assure compatibility. Participatory methodologies and tools developed within the URBiNAT project will be made available as generic manual descriptions and licensed for non-commercial use. The NBS catalogue will be integrated in the business specifications for NBS.

The availability of data for re-use depends on the specificities of the data and methods used. The same applies to data quality assurance processes. For example, a minimum scale and spatial resolution will be provided for geospatial data, as well as the currentness of the data ; a minimum range of descriptions will be set for participatory processes and participants, however, there may be local limitations as to what can be described.

The time during which NBS data will remain re-usable depends on the partners offering these solutions, to be decided when implementing the Healthy Corridors in front-runner cities. The Healthy Corridor projects and methodology will be open source after their implementation.

The usability by third parties would have to be agreed between the city, local partners, Work Package Leaders and the URBiNAT's Coordination team.

Further details will be provided in future versions of this DMP.

3. Allocation of resources

Questions to be addressed:
3.1 What are the costs for making data FAIR in your WP?
3.2 How will these be covered? Note that costs related to open access to research data are eligible as part of the Horizon 2020 grant (if compliant with the Grant Agreement conditions).
3.3 Who will be responsible for data management in your WP?
3.4 Are the resources for long term preservation discussed (costs and potential value, who decides and how data will be kept and for how long)?

3.1. Costs for making data fair

In URBiNAT, the costs for making data fair are related to the costs of the project's website and Basecamp, the collaborative platform for the project management. In addition, other costs are related to the server where the collected data about cities and research will be stored.

At this stage, it is not possible to define more precisely the costs related to the collected data since they depend on the source of information, the software and the available data provided by each city and local partner, as well as on the rights on the data that will be considered to be made public, if possible.

3.2. Coverage of costs

The costs for making data fair will be covered by the project's coordinator - CES, in the case of the website and Basecamp. Concerning the server for data storage, the costs will be covered by the partner responsible for the purchase of the server, IULM (WP5). Data stored or managed by single partners will be at their costs.

3.3. Partners responsible for data management

The following table shows who is responsible for data management in each WP.

Work package	Responsible partner	Function
WP1	Gonçalo Canto Moniz (CES)	Project coordinator (tactical)
	Denise Esteves/Begoña Dorronsoro (CES)	Research manager (operational)
	CES, ICETA-CIBIO, DTI, IULM, ITEMS, CF, IKED	Steering Committee (strategic)
WP2	José Miguel Lameiras (ICETA-CIBIO) Marco Acri (UNG)	WP leader Partner supporting Follower cities
WP3	Knud Erik Hilding-Hamann (DTI)	WP leader
WP4	Gonçalo Canto Moniz (CES) for NBS and HC	WP leader
	Chiara Farinea (IAAC) for Technological NBS	Task leader
WP5	Guido Ferilli (IULM)	WP leader
WP6	Sebastien Levy (ITEMS)	WP leader

WP7	Laura Prisca Ohler (CF)	WP leader

3.4. Discussion of resources for long term preservation

The discussion around the resources for long term preservation of data (costs and potential value, who decides and how data will be kept and for how long) is being carried out in URBiNAT by the Steering Committee, who takes decisions regarding the project's website and collaborative platform for project management (Basecamp).

Additional measures/actions will have to be agreed between the cities and the URBiNAT coordination, including the issue of physical archive and preservation of any document or data not in digital format (e.g. models, drawings, signed informed consent sheet).

Additionally, as part of the business cases developed in WP4 and WP7, for each domain, the relevant stakeholders will be encouraged to continue hosting any of the ecosystem's components locally, including the historical data and API.

The maintenance of the dataset over a period of time beyond the project's duration will also be explored through libraries, national authorities hosting relevant statistical information and public-domain online repositories like archive.org.

4. Data security

Questions to be addressed:
4.1 What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?
4.2 Is the data safely stored in certified repositories for long term preservation and curation?

4.1. Provisions for data security

URBiNAT will provide well-established communication protocols (e.g. HTTPS) to avoid eavesdropping and man-in-the-middle attacks, as well as encryption and authentication of message exchanges, protection measures (firewalls, intrusion detection, etc.) and well-defined APIs to transmit and access data.

Also, authentication will always be required to access data not fully open, based on an Authentication server that will restrict access depending on the user identity, profile and the device currently used to access. Additionally, logs of all transactions in the databases will be kept continuously and backups of the logs will be done periodically, so that actions performed upon the data can be monitored and responsibilities attributed.

All researchers working on URBiNAT and dealing with privacy-sensitive data are required to sign a statement that they are familiar with and abide by the contractual obligations of the consortium. If not included in this obligation, they will sign a statement committing themselves to make sure that such data are not provided to persons outside URBiNAT.

In the case of Basecamp, the company offers different provisions for security, that can be consulted at https://basecamp.com/about/policies/security.

In the case of the website, none of the data stored on the website are considered sensitive. The use of the third-party software will be explicit in the terms of service and privacy policy of the website (ex. Google Analytics), and in compliance with the GDPR. Website security best practices will be implemented to address security threats and ensure data integrity and protection, such as brute force attack protection, spam filtering, HTTPS/SSL secure tunneling of connections, downtime monitoring, daily backups of the entire website, secure logins with optional two-factor authentication. Clear roles with different permission levels of content access, edition and management will be defined.

In the case of the server, further details will be provided in future versions of this DMP.

4.2. Storage in certified repositories

Data will be safely stored in certified repositories for long term preservation and curation, according to the decisions to be made by the Steering Committee for data long term preservation. It will also follow the progress of discussions underway with Oppla. Other possibilities are the national repositories, Zenodo or with the European Cloud Initiative.

5. Ethical aspects

Questions to be addressed:
5.1 Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).
5.2 Is informed consent for data sharing and long term preservation included in questionnaires dealing with personal data?

5.1. Ethical or legal issues with impact on data sharing

All partners in the URBiNAT project will work in compliance with EU General Data Protection Regulation and national data protection legislation. Observers and partners involved in non-EU countries (Brazil, Iran, Oman, China and Japan), will also explicitly agree to the data protection safeguards required by EU regulation, as referred to in the Data Management Plan, the Grant Agreement and the Consortium Agreement. All partners, observers and project facilitators commit to strongly respect the individuals and their privacy at all times.

The use of Basecamp for internal communication and data sharing among partners, and particularly the protection of personal data, is regulated by the GDPR, as well as the protection of personal data from external interlocutors (e.g. subscribers of newsletter, social media).

Regarding data on the background[1] of the present partners this will be specifically regulated in the Consortium Agreement.

All research activity of URBiNAT will be developed in the EU and conducted under the EU legal framework. Nevertheless, the URBiNAT project involves partners and observers in third countries, namely in Iran, China, Brazil, Oman and Japan. Since they are all part of URBiNAT's Community of Practices aimed at sharing knowledge and experience, curated data may be exchanged between the EU-based partners and the non-EU based partners, provided that these countries comply with adequate levels of data protection (data transfers to third countries).

Apart from making data and data control central in the design of its solutions, the project will install appropriate data management principles. The consortium places paramount importance on the need to protect citizens' data and privacy. Therefore, each consortium partner agrees to comply with all respective EU regulations and main data protection principles, individually and jointly. These principles consider, but are not limited to:

- ❏ *Proportionality principle / Data minimization*: Only use adequate, relevant and no more data than strictly necessary;
- ❏ *Purpose limitation principle:* Limit data to the specified, pre-defined, explicit, legitimate initial purpose; prohibition of secondary use/use for purposes not compatible with the initial purpose;
- ❏ *Assessment*: Analysis of the proportionality between public and private interests to be protected, means to be used and prevent invasion/harm resulting from data collection;

[1] '**Background**' means any data, know-how or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that: (a) is held by the beneficiaries before they acceded to the Agreement, and (b) is needed to implement the action or exploit the results.

- ❏ *Accuracy/Reliability*: Clear distinctions between 1) personal data from i) survey participants, ii) pilot participants, and iii) third parties; and 2) degrees of accuracy and reliability of personal data (evidence, assessment, etc.);
- ❏ *Time-limited identifiable information:* Data kept in a form that allows identification of data subjects for no longer than it is necessary, for the purposes for which the personal data are processed;
- ❏ *Security of storage and access rights:* Design and implementation of appropriate measures and processes.

URBiNAT's ethics principles and guidelines will also be applied to its data management plan and, consequently, to data collection and management throughout the project.

Moreover, URBiNAT has as reference principles the human rights-based approach to data collection and use as identified by the UN Human Rights Office applied in the measurement of the implementation of the 2030 Development Agenda: the participation of population groups, in particular those marginalized in the data collection process; the disaggregation of data to prevent discrimination based on sex, age, ethnicity, disability, sexual orientation or religion, which is prohibited by international human rights law; self-identification, without reinforcing further discrimination of these groups; transparency to guarantee the right to information; respecting the privacy of respondents and the confidentiality of their personal data; and accountability in data collection and use.

Personal data collected for research purpose, i.e. data from participants, will be regulated by URBiNAT's ethical guidelines and in compliance with EC requirements. For instance, in the case of the interviews conducted in WP7, all interviewees will receive an Information Sheet, written in plain language and in the official language for each country, informing them of the use and storage of their data, and also about their rights, including to withdrawal at any time without consequences.

Data collected via online tools will be always performed avoiding the collection of any personal data of users, except if users are willing to register. In this case, the platform/website will maintain and record user information. It is important to note that prior to registration, these users will be asked to accept terms and conditions, written in accordance with the new regulation (GDPR), in order to obtain their informed consent for registration and participation/activities on the platform.

In the case of unregistered users, all data will be collected, by design, in an anonymised way to avoid the storage of any data that can be connected to any user getting in contact with URBiNAT's online tools.

In the case of social platforms, such as Facebook and Twitter, all data will be collected in an aggregate and anonymised way, by design. In regard to analytics exported and shared externally to the project, all exported data will be based on anonymously classified and logged data, not related to the user's profile or preferences.

Other ethical or legal issues with impact on data sharing may arise as a result of specificities of the data and methods used in different tasks (e.g. local diagnostic in cities, community-driven processes). These issues will be further discussed with cities and local partners during the implementation of activities. However, the Steering Committee is responsible for monitoring legal compliance and ethical issues, with the support of the URBiNAT's Ethics Commission.

5.2. Informed consent included

Informed consent for data sharing and long term preservation will be included in questionnaires dealing with personal data.

In the case of Consortium Partners and members of the Advisory Boards, their personal data will be registered and made available in contact lists shared with partners upon request and after receiving their acceptance. The request may be included in specific contact or through a specific formal agreement.

A informed consent form will be also included in the website to provide contact details for specific use, such as subscription to the project newsletter.

ANNEXES

Annex 1: EU legal framework for privacy, data protection and security

Privacy, security and data protection are interconnected rights in the EU framework, regulated by the following directives and regulations:

Charter of Fundamental Rights of the European Union (2012/C 326/02)
The European Convention on Human Rights
Directive 95/46/EC (Data Protection Directive)
Directive 2002/58/EC (Privacy and electronic communications - e-Privacy Directive)
Directive 2006/24/EC (Retention of data generated or processed)
Directive 2009/136/EC (Cookie Directive)
Directive 2016/680/EC (Protection of personal data)
European Code of Conduct for Research Integrity
Horizon 2020 Ethics Self Assessment
The European Textbook on Ethics in Research
The RESPECT Code of Practice for Socio-Economic Research
Regulation 2016/679/EC (EU) - General Data Protection Regulation (GDPR)

Personal data

The Handbook on European data protection provides important definitions for this DMP, such as:

- **"*Data*** *are personal data if they relate to an identified or identifiable person, the 'data subject'*." (p. 83);
- **Nature of the data**: "*any kind of information can be personal data provided that it relates to an identified or identifiable person*" (p. 86)

In the **Charter of Fundamental Rights of the EU**, the right to data protection is a fundamental right guaranteed under EU law: article 7 with the "*respect for private and family life, home and communications*"; article 8 with the principles on protection of personal data, such as *consent* (data may be processed only if the person gives prior consent), and *rights* to data subjects to i) have access to information about them registered in the databases, ii) rectify the data, and iii) to object to data processing in certain situations.

The **General Data Protection Regulation** (GDPR), Regulation 2016/679/EC, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, defines **personal data** (article 4, nº 1) as follows: "*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

Personal data processing is also defined as: "(...) *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (article 4º, nº 2).

It reasserts also the principles from the Charter of Fundamental Rights to be observed on protection of personal data and defines as principles for processing personal data:

- *Lawfulness, fairness and transparency* (in relation to the data subject) (art. 5, 1a);
- *Purpose limitation* (collection of data shall be specified, explicit and with legitimate purpose) (art. 5, 1b);
- *Data minimisation* (restriction of amount of data necessary) (art. 5. 1c);
- *Accuracy* (data that are inaccurate should be erased or rectified) (art. 5, 1d);
- *Storage limitation* (data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed) (art. 5, 1e);
- *Integrity and confidentiality* (security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures) (art. 5, 1f).

Personal data processing should also apply at least one of the following criteria:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (art. 6, 1a);
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (art. 6, 1b);
- Processing is necessary for compliance with a legal obligation to which the controller is subject (art. 6, 1c);
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person (art. 6, 1d);
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (art. 6, 1e);
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (art. 6, 1f).

In addition, the GDPR, on its general considerations (n. 32), defines a legal basis for consent:

- Given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her;
- A written statement, including by electronic means, or an oral statement;
- Cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them;
- If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Regarding the consent, is important to point out that the competence to define an informed consent is left to the domestic law. However the GDPR (article 4) states that : **"*'Consent'*** *of the data*

subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"

The same document (article 7) states that consent must present the following elements:

- ❏ Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data; (art. 7, 1);
- ❏ If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. (art. 7, 2);
- ❏ The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. (art. 7, 3);
- ❏ When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. (art. 7, 4).

Privacy and security

Another important concern are electronic communications, since they play a relevant role in the project, either for internal communication between partners or to disseminate information about the project on the website, social media, or through the registration of users to receive a newsletter, for example.

In order to protect issues such as confidentiality of information, treatment of traffic data and spam and cookies, the EU Directive 2002/58/EC on privacy and electronic communications (e-Privacy) distinguishes three main categories of data generated in the course of a communication:

- ❏ *Confidentiality* of the data constituting the content of the messages sent during communication;
- ❏ *Metadata* (referred to as "traffic data" in the Directive) are the data necessary for establishing and maintaining the communication, such as information about the communication parties, time and duration of the communication;
- ❏ *Location data*, within the metadata, are data specifically relating to the location of the communication device (location data), are at the same time data about the location of the users of the communication devices, particularly where users of mobile communication devices are concerned.

The Directive states that on *Security* (article 4):

- ❏ The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services;
- ❏ In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

The same directive introduces the following restrictions:

- ❑ Without previous consent, is not allowed the intrusion of privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and emails, including SMS messages;
- ❑ Without previous consent, is not allowed the setting of cookies, software that monitors and records a computer user's actions (introduced by Directive 2009/136/EC - Cookies Directive).

Annex 2: National legal frameworks

GDPR is the legal framework that EU countries should follow, transferring to their domestic law. So, currently, we have many different situations. For instance, Portugal is still discussing in its Parliament the new personal data domestic law while Italy already transferred the GDPR to its domestic law. The domestic law is important to the informed consents, for example.

Belgium

The protection of personal data in Belgium is guaranteed by the Gegevensbeschermingsautoriteit (GBA), the Belgian data protection authority. The GBA is an independent body, with powers of authority throughout the national territory. It is endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law. (https://www.dataprotectionauthority.be/)

The principal data protection legislation in Belgium is the Regulation 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) as this is immediately applicable in law as a regulation. Next to this, the Belgian Parliament has approved the Law on the protection of individuals with regard to the processing of personal data on July 30 2018, which clarifies and regulates certain areas as stipulated in the EU regulation. This law was published on 5 September 2018, at which date the law went into effect.

In addition, as a federal state, the Belgian and Flemish legal framework includes other laws and decrees impacting data protection, especially concerning the electronic communications sector and financial companies.

Bulgaria

The Constitution of the Republic of Bulgaria safeguards citizens' rights and states that privacy is inviolable. In addition to the rules in Chapter Two, explicit provisions on data protection are not detected. In accordance with the Constitution, the protection of personal data in Bulgaria is implemented through the provisions of the Protection of Personal Data Act adopted in 2002. Since the adoption of EU Regulation 2016/679, a draft law amending and supplementing the Personal Data Protection Act has been developed to transpose the provisions of the Regulation into the national legislation. The draft of this Act is due to be discussed at second reading by the Members of the Parliament and adopted accordingly. Meanwhile, the Personal Data Protection Commission adopts opinions related to the implementation of Regulation 2016/679.

The Classified Information Protection Act (CIPA) introduces very clear restrictions on access to Classified Information. For the purposes of the CIPA, "classified information" is any information which is a secret or an official secret, and any foreign classified information. The unauthorized access to such information, which may threaten or prejudice such interests of the Republic of Bulgaria as regards national security, defense, foreign policy or protection of the constitutional order, shall be prohibited. Clarifications on the nature and the content of the state secret information is provided in additional appendix (Schedule 1). Such unauthorized access is likely to

have an adverse effect on the interests of the State or any other interest protected by law. The Official secret information is generated or stored by government authorities or by the authorities of local self-government, is not a State secret, and the unauthorized access to which might adversely affect the interests of the State or prejudice another interest protected by law.

At the local administrative unit level (LAU)[2] and at district level[3] information about the population can be derived from the registers of the Unified System for Civil Registration and Administrative Service of the Population (further divided into smaller units). The rules for the System's operation and access to information are defined by the Civil Registration Act. Article 106 of the Civil Registration Act provides for a special order for access to data from the System, and instructs that this information is accessible for state bodies and institutions only on the basis of their statutory powers. Officials from the municipal administrations carrying out civil registration activities can provide such data. There is no explicit provision on the access to data for the purposes of scientific and research projects. No rules have been laid down for the provision of information already obtained by the System of Rights holders and already kept by third parties.

One of the main sources of information about the city and its inhabitants is the information collected by the National Statistical Institute. The Institute's rules on the collection and provision of information are governed by the Statistics Act. Chapter Six of the Statistics Act introduces the requirements for statistical confidentiality. Article 25 states that "Individual data collected and those collected through statistical surveys shall constitute a statistical secret and may only be used for statistical purposes."

In this regard, the National Statistical Institute and its staff may not disclose or provide:

- ❏ individual statistical data;
- ❏ statistical data which can be matched in a way that enables the identification of a specific statistical unit;
- ❏ statistical information which aggregates data about less than three statistical units or about a population in which the relative share of the value of a surveyed parameter of a single unit exceeds 85 per cent of the total value of such parameter for all units in the population.

An opportunity to access individual anonymous data for scientific research purposes is granted to higher schools or legal entities with the permission of the President of the National Statistical Institute provided that the application does not conflict with Article 25 cited above.

Access to data at individual territorial levels is strongly related to the methodology of producing information on the relevant indicator. Information on low territorial levels for the population and the housing stock is available from the Census Survey 2011. It could be used in cases when the rules for the statistical confidentiality are closely followed.

The Access to Spatial Data Act transposes the European Directive 2007/2 / EC INSPIRE into Bulgarian legislation. This law governs the maintenance and use of infrastructure for spatial information, the provision of access to spatial data and the provision of services for environmental data or activities that may have an impact on the environment by ensuring compatibility and security in the exchange of data. The Act provides the rules governing the establishment of an

[2] Covers the territory of Sofia municipality and includes both urbanized and non-urbanized territories. Corresponds to LAU 2-level until 2016.

[3] Sofia municipality is divided into 24 districts. The mayors of the regions resolve problems arising from the daily needs of the population at the place of residence, administrative services of the citizens, development, cleaning and maintenance, etc.

infrastructure for spatial information, the provision of access to spatial data and the provision of environmental data services or activities likely to have an impact on the environment, by ensuring compatibility and security in the exchange of data. Chapter Three describes the services for spatial data and metadata and the procedures for access to them. The foundations of the National Spatial Data Portal (http://www.inspirebg.eu/) have been laid. As for 2018, the portal currently works with a limited number of topics and the information is limited to the national level.

The information on the location, boundaries and dimensions of the real estate on the territory of the Republic of Bulgaria is maintained by the Cadastre and Property Register. Issues related to the organization, financing, creation, management and use of the cadastre and the property register are regulated by the Cadastre and Property Register Act. The Agency for Geodesy, Cartography and Cadastre shall provide upon request services related to data from the cadastral map and the cadastral registers by providing official documents and reports in electronic form and / or in written and graphic form against which they receive payment at certain tariffs. When providing data and services from the Agency, personal data is limited.

In addition, the Bulgarian legal framework includes other laws and decrees related to data protection, especially concerning the electronic communications sector (Electronic Communications Act), health status of individuals (Law of Health) the financial sector and the financial intermediators.

Denmark

Data protection rules and principles in Denmark as of 2016 include obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data.[4]

The Danish Data Protection Act has been passed by the Danish parliament. The GDPR and the Danish Data Protection Act repeal the Danish Personal Data Processing Act as of 25 May 2018.

The Danish Act has supplementary provisions to the GDPR on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.[5] In broad outlines the Act covers the following issues:[6]

- ❏ fines to public authorities;
- ❏ processing personal data as part of HR-administration;
- ❏ disclosure of personal data for marketing purposes;
- ❏ exceptions to the duty of disclosure and the right of access;
- ❏ designation of a data protection officer (DPO) ;
- ❏ the category of semi-sensitive personal data is left out;
- ❏ moderation of the so-called "rule of war" which according to the old Data Protection Act implied that larger public registers containing personal data must be stored in Denmark;

[4] For further details, namely regarding national regulator, its enforcement powers, and sanctions and remedies, see: https://uk.practicallaw.thomsonreuters.com/6-619-2165?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1#co_pageContainer

[5] See Data Protection Act: https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf

[6] See broad outlines or main highlights of the Danish Data Protection Act and the GDPR: https://www.twobirds.com/en/news/articles/2018/denmark/the-danish-data-protection-act-has-been-passed

- ❏ social security numbers;
- ❏ processing of data concerning criminal offences;
- ❏ age limit for consent to use information society services;
- ❏ deceased persons;
- ❏ TV monitoring;
- ❏ the limitation period for infringements of the GDPR and the Danish Data Protection Act is 5 years;
- ❏ combination of data for control purposes in public registers is removed;
- ❏ credit rating agencies and warning registers;
- ❏ notification to the Danish Data Protection Agency on warning registers, credit rating agencies and judicial information systems;
- ❏ the rules concerning transferring to archives in accordance with the archival legislation are re-enacted;
- ❏ public authorities processing for a new purpose is extended;
- ❏ prohibition on transfers of sensitive data to third countries;
- ❏ the Danish Data Protection Agency with a council and a secretariat is re-enacted;
- ❏ mass media and the freedom of speech, is not subject to the Data Protection Act;
- ❏ administrative penalties.

The Danish Law on the handling of personal data by law enforcement authorities can be consulted at the following link: https://www.retsinformation.dk/pdfPrint.aspx?id=189891

France

The Data Protection Act (Loi Informatique et Libertés) and its implementing decree have been amended to bring national law into line with the European legal framework. These texts allow the practical implementation of the General Data Protection Regulation (GDPR) and the "police-justice" Directive, applicable to criminal records. The readability of the national legal framework will be improved by an ordinance to be issued within the next six months[7].

The Commission Nationale de l'Informatique et des Libertés (CNIL) is expected to propose new regulatory tools allowed by the GDPR or the amended law:

- ❏ the upcoming adoption of 3 "referentials" relating to customer management, human resources and health vigilance. These standards update the CNIL's doctrine with regard to the new requirements of the GDPR, based on the original doctrine (single authorisations, simplified standards, compliance packs, etc.);
- ❏ a "standard regulation" on biometrics has been in consultation since September 3. It will make it possible to set a demanding and protective framework;
- ❏ a first certification procedure is in the finalization phase: a public consultation was launched and closed at the end of June on the "DPO" certification (176 contributions received). The standards will be finalized in September.

Italy

[7] See CNIL: https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application

Italy´s consolidated data protection code came into force on 1 January 2004 (Data Protection Code - Legislative Decree no. 196/2003). The Code brings together all the various laws, codes and regulations relating to data protection since 1996.

In particular, it supersedes the Data Protection Act 1996 (no. 675/1996), which had come into effect in May 1997. The code was recently amended by the decree adapting the national legal system to the GDPR 2016/679 (Legislative Decree No. 101 of 10 August 2018).

Accordingly, several of its provisions were amended or repealed and sections were added. The decree has made use of the margin of manoeuvre afforded by the GDPR to Member States as regards, in particular, processing activities based on legal obligations or for purposes in the public interest (Article 6(1), letters c) and e)); processing of biometric, genetic and health-related data (Article 9(4) and Article 36(5)); processing activities covered by Chapter IX of the GDPR (journalism, labour, research, archiving, etc.). As a result, several provisions of the 2003 Code were left in place as they were found not to be in conflict or overlap with the GDPR and to provide added value for the relevant stakeholders based on the implementing experience of the past 15 years.

In 1997, when the former Data Protection Act came into force, was established the Italian Data Protection Authority (Garante per la protezione dei dati personali), by the so-called privacy law (Law No. 675 of 31 December 1996) and regulated subsequently by the Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003), as amended by Legislative Decree No. 101 of 10 August 2018, which also established that the Italian DPA is the supervisory authority responsible for monitoring application of the General Data Protection Regulation (pursuant to Article 51 of Regulation No. 2016/679).

The Italian Data Protection Authority is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals' dignity. It is a collegiate body including four members, who are elected by Parliament for a seven-year term. The authority has an office in Rome with a staff currently numbering about 125 people. The tasks of the Garante are laid down in the Personal Data Protection Code (legislative decree No. 196/2003) as well as in other national and EU regulatory instruments.

The Garante works to ensure that, in all public and private sectors, data are processed as required by the law and the rights of individuals are respected whenever their personal data are processed.

The main tasks of the Garante are:

- ❏ check that personal data are processed in line with laws and regulations and, where appropriate, we order data controllers and data processors to take specific measures in order to process the data according to the rules;
- ❏ handle complaints;
- ❏ ban, in whole or in part, or order the restriction of the processing of personal data if the nature of such data or the mechanisms or effects of the processing may substantially affect data subjects;
- ❏ take the measures envisaged in data protection legislation;
- ❏ draw the attention of Government and Parliament, wherever appropriate, to the need for passing specific laws or regulations in various walks of life;
- ❏ participate in the debates on law-making activities through hearings before Parliament;
- ❏ issue opinions;
- ❏ draw up an annual report of our activities and the current enforcement of privacy legislation, which is submitted to Parliament and Government;

- ❏ participate in data protection-related activities at EU and international level, and we also carry out supervisory and support activities regarding Europol, Schengen, VIS and similar information systems;
- ❏ raise citizens' awareness of personal data protection issues and data security measures;
- ❏ seek the involvement of citizens and stakeholders via public consultations whose findings are taken into account in drafting general application measures.

Portugal

The Constitution of the Portuguese Republic of 1976 specifically addresses, in its article 35, the "use of information technology" in relation to data protection. In addition, the Portuguese legal framework include other laws and regulation impacting data protection, especially concerning the electronic communications sector and financial companies.

The protection of personal data in Portugal is guaranteed by the *Comissão Nacional de Protecção de Dados* (CNPD - National Commission on Data Protection), the Portuguese data protection authority. The CNPD is an independent body, with powers of authority throughout the national territory. It is endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law.[8]

The principal data protection legislation in Portugal is the law 67/98 of 26 October 1998 ("Data Protection Act"), which transferred into the Portuguese legal system the directive 95/46/EC on the protection of personal data and on free movement on such data. In order to implement the GDPR in Portugal, the Portuguese government submitted to the Portuguese Parliament a draft law (law 120/XIII), which is still under evaluation.

Slovenia

The protection of personal data in Slovenia is regulated by the General Data Protection Regulation (Government Gazette of the Republic of Slovenia 94/07). The currently valid text is available on the link: http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906

The General Regulation (Regulation 2016/679) sets out uniform rules for the protection of personal data in the EU, and some substantive and procedural issues can be specifically regulated by the Member States. This will be regulated by the new General Data Protection Regulation. The new proposal of the legal document to be aligned to the European Union directives is currently in the legislative process, being expected for 2018.

At present, the obligation for data processors are the following:

- ❏ to report personal data filing systems to the register managed by the Information Commissioner;
- ❏ to assure effective protection of personal filing systems,
- ❏ to adopt a more detailed internal regulations governing the protection of personal data;
- ❏ prior to the start of video surveillance to post a visible notice to this end,
- ❏ prior to the start of video surveillance to acquire opinion from the syndicate representatives;

[8] https://www.cnpd.pt/english/index_en.htm

- ❏ prior to the start of biometric measures, the employees must be notified in writing and the Commissioner must issue a decision to this end;
- ❏ in case when two or more filing systems are being linked the Information Commissioner must be notified;
- ❏ in case when sensitive personal data is being linked the information Commissioner must issue a decision to this end;
- ❏ in case the data is being transferred to third countries the information Commissioner must issue a decision to this end.
    - Contractual Clauses for the transfer of personal data to third countries, under Directive 95/46/EC, Commission Decision;
    - Contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, Commission Decision;
    - Alternative set of standard contractual clauses for the transfer of personal data to third countries, Commission Decision of 27 December 2004 amending Decision 2001/497/EC;
    - Standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, Commission Decision of 5 February 2010.