Project number: 7123420

LEARNING LOOPS IN THE PUBLIC REALM

WP2. Data collection and visualisation framework
T2.4. Development of the legal framework

Deliverable D 2.2

Report on the legal and regulatory frameworks applicable to data collection in living labs

Version: 1.0

Date: 13th May 2018

Responsible partner: Vrije Universiteit Brussel

Authors: Eugenio Mantovani

The project is supported by the Brussels Capital Region – Innoviris (Belgium), Ministero dell'Istruzione dell'Università e della Ricerca (MIUR) (Italy), the Economic and Social Research Council (UK) and the European Union.

DOCUMENT CHANGE RECORD

Version	Date	Status	Author	Description
0.1	09-03-18	Draft	EM (VUB)	Draft for internal discussion
0.2	26-03-2018	Draft	Imre Keseru (VUB)	Comments on whole draft
0.3	26-04-18	Draft	Massimiliano Condotta (IUAV)	Review, comments request to add new annex
0.4	05-05-18	Final draft version	Eugenio Mantovani (VUB)	Final draft version
0.5	07-05-2018	Final draft version	Imre Keseru (VUB)	Formatting, typos, references
1.0	13-05-2018	Final version	Eugenio Mantovani (VUB)	Final version for consortium review

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

1.1. The project LOOPER and the LOOPER Living Labs

The aim of the LOOPER project is to build a participatory co-creation methodology and platform to demonstrate 'learning loops' i.e. new ways of decision-making which bring together citizens, stakeholders and policy-makers. In short, a typical LOOPER loop starts with debate on topical issues, then frames the problem and collects data using participatory sensing techniques and technologies. The platform then visualizes the data and enables the co-design and evaluation of solutions using both online and physical participation tools. The selected solutions are then implemented, and the results are monitored with a second loop learning from the first.

The methodology and the prototype platform are to be tested in three concrete urban settings. The LOOPER Living Labs (LLLs) target different spatial, cultural and thematic contexts: mobility in Brussels; air quality, traffic safety, community spaces in Manchester; environmental pollution in Verona.

1.2. Citizens' participation: physical and online meetings, participatory sensing, and geotagging

As these introductory remarks indicate, LOOPER is based on the active participation of citizens and urban stakeholders, such as municipalities, regional agencies, associations. The citizens' active involvement and contributions are expected at three levels:

First, the project foresees the physical participations of citizens in regular meetings where the topical issues are discussed.

Second, in LOOPER, participants will discuss co-design alternatives and vote for alternatives online, using the LOOPER platform. In doing so, citizens will be able to engage in the process of adding photographs, videos, comments, to the geographical area or areas that are intentioned by the living lab or to add geographical information to digital content (geotagging).

Furthermore, the project foresees the involvement of citizens in the process of collecting data about the environment they live in. For this activity, sometimes referred to in the literature as "participatory sensing" or "participatory monitoring" (Goldman et al., 2009), citizens collect data about air quality, temperature, traffic, etc. The process begins after citizens/participants have determined the goals of the data collection and a plan for collecting data. Participants collect data automatically (e.g., location logging) or manually (e.g., taking pictures), using mobile phones or other mobile or fixed devices. Data is then transferred via wireless infrastructure to a data repository. The data is then processed and analysed; the results of analyses are visualized and can be used to support decisions.

The participation in physical meetings, the discussion of co-design alternatives and voting for alternatives online, and the active involvement of citizens in "sensing" the environment they live in, entail an active engagement of physical persons and the collection and processing of data, including personal data.

1.3. Objective and structure of this deliverable

The main objective of this deliverable is to map, explain, and to provide guidance to partners, in the implementation of the personal data protection legislation in the LOOPER project in general and for each LOOPER Living Lab in particular. Section 2 illustrates the types of data, including personal data, which are planned to be collected and processed in LOOPER. In order to ensure that research activities are in line with the law and with the rights and expectations of individuals, the relevant legal framework is illustrated in section 3. Subsequently, the deliverable discusses the impacts of LOOPER and of the LOOPER living labs on those frameworks (section 4). A table at the end of this document draws up a list of recommendations for LOOPER partners (section 5).

1.4. Links with other deliverables

Deliverable D2.1 Report on data collection procedure framework describes the tools to properly collect the data they need, and to create and implement the visualization of all data in order to have a clear and complete vision of the situation. While that deliverable addresses technical feasibility and options, the present complements it by addressing the legal framework for conducting the data collection and processing activities foreseen therein.

The development of an integrated framework for implementing, monitoring and evaluating the urban living labs, is the objective of WP4. Deliverable 4.1, in particular, develops guidelines to engage citizens and other key stakeholders in the living labs. This deliverable adds to the description of methods, technologies, case studies and users provided in that document by offering a view on the legislative framework for the data processing activities foreseen in the living labs.

In addition, this document implements the indications contained in D1.1 - Quality Management Plan, paragraph 6 “Ethical and regulatory considerations”. This section of D1.1, in essence, poses two demands on the project: on one hand, to ensure that the personal data processing activities that will take place in the course of the project respect personal data protection law. This demand is addressed in the present deliverable D.2.2. On the other, deliverable 1.1 asks from the project to think and make a plan to take into consideration gender aspects and the needs of hard-to reach and vulnerable groups, especially the elderly, the poor, the marginalised youth and persons with disabilities. These demands will be addressed in Deliverable D3.2.

2. DATA, INCLUDING PERSONAL DATA, PROCESSED IN LOOPER

The collection and the processing of personal data in the LOOPER project is limited to the following categories of personal data and simple (not personal) data:

1. Name, surname, affiliation, of researchers coming from the organisations involved in the project;
2. Name, surname, affiliation, and professional opinions of individuals who, in their personal capacity or as representative of the organization of affiliation, will participate in the project as invited speakers.
3. Name, surname, and email address of citizens/research participants taking part in LOOPER living labs;
4. Access logs containing IP addresses of citizens/research participants in online discussion and voting through LOOPER platform;
5. Geo-localised data collected during the phase of participatory monitoring or sensing;
6. Environmental publicly available information (not personal data).

For descriptive purposes, these types of personal data can be divided into three categories.

2.1. Identification data of participants in the project

The project is based and encourages active participation of citizens. Given the scope and nature of the project, participants are expected to use their real names when they participate in physical meetings and in online activities and to freely express their opinions.

The project partners also register name, surname, and email address researchers coming from the organisations involved in the project and of individuals taking part occasionally as experts.

This personal information is contained in lists of participants drawn for each LOOPER Living Labs.

2.2. Access logs and IP addresses of citizens

When they engage in the online activities, e.g., discussion or voting alternative solutions, individuals leave behind personal data, notably their IP addresses, and also usernames, that can be linked to them.

In discussions online, individual may also unwillingly disclose personal sensitive information about themselves or others.

This personal information is recorded by the access logs memory of the Looper collaborative platform. Other personal information may be accessible on the platform discussion *fora,* such as location data after geotags.

2.3. Location data and other data collected through participatory sensing and geotagging

The citizens who participate in the project will use sensors embedded or associated with mobile smartphones: The Air Beam or Air Casting devices for air pollution measurements and the noise tube for noise measurement, for instance, or geotagging devices (see D2.1).

These devices are carried by citizens / research participants. As participants move in the area of the living lab, the sensors placed in the mobile devices collect data about air pollution levels, noise, and other environmental information, such as road safety / parking or public greenspaces (See D4.1 Guidelines for Living Labs).

In addition, using geotagging functionalities, participants can take pictures of particular areas (e.g., a crossing point) and upload it to the LOOPER platform. This means users share their location information with the same post on the project platform. As planned in D2.1, Section 3, there will be a direct link to

the external application for the geotagging [...] data collected with this tool will be stored in the main LOOPER platform geo-database via a scheduled automatic upload procedure.

2.4. Environmental publicly available information

During the project, LOOPER researchers and participants will collect environmental information, mostly from stationary surveys (See D2.1). Environmental information includes any information in any form or format about the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape etc. or factors, such as substances, energy, noise, radiation or waste, or measures (including administrative measures), such as policies, legislation, plans, programmes, reports.

Information about the environment is not subject to personal data protection law. This type of information is publicly available, meaning that any citizen has the right to access it (See below 3.2 and 4.9 on Directive 2003/4/EC on public access to environmental information).

3. THE RELEVANT LEGAL FRAMEWORKS

The relevant legal frameworks for LOOPER research activities include the data protection legislation, legislation on the processing of personal data in the electronic communications sector, and legislation on the publicly available environmental information.

3.1. The personal data protection legislative framework

At the European level, legal protection of personal data is enshrined in article 8 of the European Convention on Human Rights (ECHR) and in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108).

In the European Union, the protection of personal data is recognised in the Charter of the Fundamental Rights (CFR), article 8, and in article 16 Treaty on the Functioning of the European Union (TFEU), which recognises that "[e]veryone has the right to the protection of personal data concerning them" when the EU or Member States carry out activities which fall within the scope of Union law, and article 39 of the Treaty on European Union (TEU), according to which "the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data."

The EU constitutional provisions are further specified in secondary legislation. The centrepiece legislation is the General Data Protection Regulation or GDPR (Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data), which will apply from May 25th, 2018, repealing the incumbent 1995 Data Protection Directive (Directive 95/46/EC). The objective of the Regulation is stated in art. 1 (2), *viz.* the protection of "the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data."

In addition, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications or e-privacy Directive), currently under revision, applies. The provisions of this Directive specify and complement the EU data protection regulation, providing an equivalent level of protection in Member States with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

In addition, the legal framework includes national legislations in force in the jurisdictions involved in the project, namely:

a) The Privacy Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, for Belgium, https://www.privacycommission.be/en/privacy-act and the Wet betreffende de elektronische communicatie/Loi relative aux communications électroniques) of 13 June 2005 (eCommunications Law), as amended by the Law of 28 June 2012, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2005061332, for Belgium;
b) The Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196), including "Titolo X" of the Codice (artt. 121-134) which contains the implementation of Directive 2002/58/EC, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 , for Italy;
c) The Data Protection Act of 1998 https://www.legislation.gov.uk/ukpga/1998/29/contents and the Privacy and Electronic Communications (EC Directive) Regulations 2003 https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/ , for the UK.

For the purpose of this project, the data protection framework is squarely derived from the EU Regulation and the e-privacy Directive, save for national idiosyncrasies that are addressed specifically, if any.

Given the European scope of the project, the EU Regulation and the Directive applies also in the UK, a state which is the process of withdrawing its membership from the European Union ("Brexit"). (EU Commission 2017).

3.2. The EU directive on access to environmental information

Data protection law does not apply to environmental information.

The relevant legal framework is provided in the EU directive on access to environmental information (Directive 2003/4/EC on public access to environmental information). Directive 2003/4/EC provides that any individual has the right to access environmental information held by public authorities. Accordingly, the Directive specifies the obligations of public authorities to provide access to environmental information.

Public authorities which fall under the obligation to provide access are, according to the Directive, government or other public administration, including public advisory bodies, at national, regional or local level, any natural or legal person performing public administrative functions under national law, including specific duties, activities or services in relation to the environment; and any natural or legal person having public responsibilities or functions, or providing public services, relating to the environment under the control of a government body or administrations (art. 2.2 Directive 2003/4/EC).

The foregoing applies to the public authorities involved in LOOPER Living Labs.

According to recital 14, public authorities should make environmental information available in the form or format requested by an applicant unless it is already publicly available in another form or format or it is reasonable to make it available in another form or format.

In addition, public authorities should be required to make all reasonable efforts to maintain the environmental information held by or for them in forms or formats that are readily reproducible and accessible by electronic means. This information must be provided within one month of a request (art. 3.2 Directive 2003/4/EC).

The Directive foresees a series of exceptions, to be interpreted narrowly, in which requests to access information can be refused (art. 4 Directive 2003/4/EC).

3.3. The EU General Data Protection Regulation

The centre-piece legislation applicable to personal data processing activities carried out within the LOOPER project is the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). The regulation includes definitions, principles, legitimate basis for processing personal data, rights of data subjects and obligations of data controllers. The e-privacy directive 2002/58/EC applies for the processing of location data.

3.4. Definition of personal data and location data

The definition of "personal data" is provided in art. 4 (1) of the EU General Data Protection Regulation: "'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;."

Where data cannot be linked to a specific individual it will not be classed as 'personal data' and thus will not fall within the purview of personal data protection laws. In contrast, any processing activity involving personal data must be carried out in compliance with EU and national data protection legislation.

Included in the definition of personal data of an identifiable natural person is a reference to "location data". This provision must be read in the light of article 2, letter c of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the e-privacy Directive), which defines location data. Location is "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*."

3.5. Principles of data protection law

- **Data minimisation and purpose limitation** – This fundamental principle of data protection is an expression coined by legal doctrine to refer to two key data protection principles, namely, the purpose limitation and the data quality principles (Bygrave, 2002). The purpose or use limitation, or purpose binding principle prohibits further processing which is incompatible with the original purpose(s) of the collection (art. 6 Directive 95/46/EC). The data minimisation principle must act as a general principle policy for any technological development: information systems and software shall be configured by minimising the processing of personal data. The purposes for which personal data are collected should be specified at the time of collection. In addition, the use of those data should be limited to those previously defined purposes.
- **Fairness, lawfulness and transparency of processing** – Data subjects (citizens participating in LOOPER) should be able to know what information has been collected about them, the purpose of its use, who can access and use it. To achieve this the transparency of the data processing should be ensured. Data controllers should be clearly identified and be able to respond to requests of e.g. data subjects. Controllers must inform data subjects before the processing of their personal data about the main components of the processing (e.g. purpose of processing, identity and address of the controller, etc.).
- **Accuracy of data** – This principle implies that data must be adequate, up to date, relevant and not excessive for the purposes for which it is collected. Irrelevant data must not be collected and if it has been collected it must be discarded (Art. 6 (1) c) Directive 95/46/EC; art. 5 GDPR).
- **Storage limitation** – In principle data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data were collected or for which they are further processed. Where possible data should be pseudonymised or anonymised (art.6 GDPR).
- **Secure data** – appropriate technical and organisational measures should be taken into consideration when personal data is processed in order to ensure the 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.

3.6. Legitimate basis for processing

According to article 6 of the GDPR, personal data should be processed for one of the following reasons:

- Freely given, specific and informed consent of the data subject
- Performance of a contract to which data subject is a party
- Compliance with the legal duties of the controller
- Protection of the vital interests of the data subject
- Activity carried out in the public interest or exercise of official authority
- Legitimate interest pursued by the data controller

As the LOOPER project processes personal data based on the consent of the data subject, this section will provide a more detailed explanation of consent.[1]

Consent as a legal basis of processing personal data has three building blocks:

- Data subject must give consent freely, without undue pressure. The consent is freely given "if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent" (art. 29 WP, 2011).
- Data subject must be duly informed about the consequences of giving consent. To have sufficient information, data controller, the natural or legal person in charge of the processing (see below), must provide information in an easily understandable language.
- The consent must be specific, reasonably and relate to the reasonable expectations of an average data subject.

3.7. Rights of data subjects

As anticipated, EU data protection law recognises a number of subjective rights for data subjects, who are identified or identifiable natural person.

- **Right to be informed** – according to art. 12 GDPR the controller shall take appropriate measures to provide any information „to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means."
- **Right to access** – „the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data…" (art.15 GDPR).
- **Right to rectification** – According to art. 16 „the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."
- **Right to be forgotten** - The right to be forgotten (art. 17 GDPR) will grant the right to the data subject to have his personal data erased: *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay"*. The provision has an apparent effect in online environment since search engines must remove search results upon the request of the individual. Although it will be a newly expressed right in the GDPR, due to the decision of the Google Spain case, it is also derivable from the Directive (European Court of Justice, Google case, 2012).
- **Right to data portability** – According to art. 20 „the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided."
- **Right to object** – Art. 21 elaborates on the right to object: „The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her." Data subject has the right to object not only relating to his or her particular situation, but against profiling or direct marketing purposes as well.

[1] The description of consent is found in article 7 GDPR and in various recitals (32, on conditions for consent, 33, on consent to certain areas of scientific research, 42 on burden of proof and requirements, 43 on freely given consent)

- **Right to a judicial remedy and the right to receive compensation** - where the data subject considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation, he or she has the right to an effective judicial remedy and the right to receive compensation (art,79 GDPR).
- **The right to restriction of processing** - This right will be a new form of exercising data protection rights. Data subjects will be able to affect the extension of the data processing by claiming its restriction. Based on art. 18 (2) the conditions of restricted processing will be strict. Although it seems a technical solution, it will provide an interlocutory treatment of risk, while the data subjects decide the actual treatment.
- **Stakeholder engagement** - The Regulation also provides a platform for data subjects to be heard: Art. 35 (9) says the controllers shall seek the views of data subjects on the processing operation. The engagement of external stakeholders to the development phase has a pivotal role in impact assessments.

3.8. Obligations of data controllers

"Data-controller" is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. (art. 4 GDPR). With the GDPR, the European legislator has consolidated, in art. 24 (responsibility of the controller), the principle commonly referred to as the principle of accountability (article 5.2). The implementation of this principle falls on the shoulders of data controllers, who are under a series of obligations designed to *"ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation".*

- **Record of processing activities** – The Regulation requires a detailed documentation about the processing operations conducted by the data controller and by the processor (if any). The maintenance of the record of the activities is crucial to e.g. respond to enquiries by data subjects. (art.13 and 14 GDPR).
- **Data Security Technical and organisational measures**– The controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (art. 32 GDPR). "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed." (art. 32.2 GDPR). According to the Article 29 Working Party, these technical measures should convert 'the currently punctual requirements into a broader and consistent principle of privacy by design.' (Art. 29 WP, 2009).
- **Personal data breach notification** –If a personal data breach occurs, the controller has to assess it and shall (in certain cases) notify the supervisory authority only or the data subjects as well (art.33 GDPR).
- **Transfer of data**. The general rule regarding the transfer of personal data across national borders is that it is permissible within the EU or with other countries outside EU that provide similar, adequate level of protection. Personal data, however, cannot be outsourced to third countries without the country having an adequate level of data protection and applying a set of EU standards and specifications.

4. DATA PROTECTION IMPACT ASSESSMENT

This section assesses the impacts of the personal data processing activities foreseen in LOOPER against the conditions and requirements of fair processing of data protection law just outlined. As discussed in section 2, in the context of LOOPER, the personal data that can be processed in LOOPER living labs concerns

1. Name, surname, and email address of citizens, researchers and experts taking part in the LOOPER living lab;
2. IP addresses and other personal information provided in discussion and voting online platform;
3. geo-localised data collected during the phase of participatory sensing and geo tagging (images, comments);

Importantly, this assessment must be updated if new categories of data or new data processing activities, other than those identified in section 2, unfold. The right to access to environmental information is treated separately.

4.1. Purpose limitation, data minimisation, transfer of data

As the project is interested and concerned with public spaces, the main purpose of any data processing activities in LOOPER is to collect information about the environment and the topical issue, such as air pollution reduction, traffic mitigation, that is at stake in each living lab and learning loop.

The purpose of these processing activities is not to collect personal data about research participants or to build profiles of participants. For instance, for the purposes of the project, it is necessary to trace the location of the devices only in so far as this allows to obtain a granular visualisation of the topical issue tackled by each learning loop, e.g., areas where levels of pollution are particularly high, or where noise is above limits.

In line with the data protection principle of *data minimization* (see section 2.2), the personal data of research participants must be processed only when "required" that is, when this data is strictly "indispensable". In the context of LOOPER, the collection of personal data is necessary or "required" only in so far as it enables the mapping of the environment or a better appreciation of the environmental conditions related to the problem discussed within each Living Lab.

Any processing activities performed by LOOPER data controllers (see below) must minimise the processing of personal data of research participants to what is required to attain this specific, project's related, purpose.

Secondary uses of personal data are forbidden, unless consent is provided, or the data are fully anonymised.

The collection of other personal data, other than those mentioned in Section 3, is forbidden, unless a legitimate basis for processing such data exists. For instance, it could be useful to obtain data about health status to assess the impact of air pollution mitigating measures. This option is absolutely precluded to LOOPER, because this processing is not necessary to attain the purpose of the project. The same applies to the collection of any other personal data that may appear "useful".

No data will be transferred outside the EU.

4.2. LOOPER basis for processing personal data: Consent

As discussed in section 3, the processing of personal data must be based on a legitimate basis. In the context of LOOPER Living Labs, the legal basis for processing personal data of participants is informed consent. As discussed earlier in the Introduction, three groups of research participants are foreseen.

Participants in LOOPER include, first, researchers coming from the organisations involved in the project. These researchers participate in the project voluntarily as part of their professional activities. In line

with the European scope of the reject, LOOPER researchers are bound by European Code of Research Integrity, for what concerns the duty of confidentiality and standards of research integrity.[2]

Second, individuals may be invited to participate in LOOPER public meetings as experts. They will be asked to sign a confidentiality statement and be informed about how their personal data are treated by the consortium. Personal data to be collected and processed will include: name, surname, affiliation, and professional opinions. Participants will be fully informed, before participation, about:

1. the type(s) of data to be collected;
2. the method(s) of collecting data and opinions expressed;
3. the identity and the contact details of the data controller;
4. the purposes and legal basis for the processing;
5. the recipients of the personal data;
6. the rights to: request from the controller access to and rectification or erasure of personal data
7. confidentiality and anonymity conditions.

Third, citizens and research participants. Participation in LOOPER meetings is an essential aspect of the project, which seeks to involve the citizens in co-decisions about areas or issues falling in the public realm.

At the beginning of each Living Lab, participants will sign a consent form, after being fully informed about the following:

1. the project and the voluntary character of participation in the living lab;
2. the type(s) of data to be collected, namely, identification data and location data for those who will use the mobile sensors;
3. the method(s) of collecting data and opinions expressed;
4. the identity and the contact details of the data controller;
5. the purposes of the processing and the recipients of the personal data collected;
6. the national law regulating the processing of the personal data;
7. the rights to: request from the controller access to and rectification or erasure of personal data;
8. confidentiality and anonymity conditions.

Importantly, citizens who participate in the "participatory sensing" and geotagging activities must be informed and trained by the data controllers before they start any measurement.

See below for the content of the information obligation falling on LOOPER data controllers.

A template informed consent is provided in Annex I.

Specific information requirements must be met when using location or geotagging technologies.

See Annex II.

4.3. LOOPER data controllers

As discussed earlier in section 3, the accountability of data controllers is an essential aspect of data protection law. The recognition of data subjects' rights entails corresponding obligations incumbent on data controllers, which are the partners which have knowledge of the purpose and the means of the processing and have the closest link with participants' data (section 2.5. above). For this reason, it is

[2] The European Code of Conduct for Research Integrity, Revised edit, Berlin: ALLEA - All European Academies, 2017. http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

sensible to clearly identify the natural or legal person that acts as data controller for the LOOPER personal data processing activities.

In the LOOPER research project, each living lab has one data controller:

- For Verona LL
  Name and surname: Chiara Martinelli - Legambiente, civil society organisation, (LA)
  Address: Via Don Gaspare Bertoni n° 4 37122 – Verona
  Email contact: chiara@legambineteverona.it
- For Brussels LL
  Name and surname: Imre Keseru, VUB
  Address: Pleinlaan 2, 1050 Brussels
  Email contact: imre.keseru@vub.be
- For the Manchester LL
  Name and surname: Joe Ravetz, UoM
  Address: The University of Manchester - Oxford Rd Manchester - M13 9PL
  Email contact: joe.ravetz@manchester.ac.uk
- For the information collected and processed in the project's platform and web site the data controllers are
  - IUAV – for data collected in the participatory sensing or monitoring activities
    Name and surname: Massimiliano Condotta
    Address: Dipartimento di Culture del progetto Dorsoduro 2196, Cotonificio veneziano 30123 Venezia
    Email contact: condotta@iuav.it
  - VUB – for data about LOOPER website
    Name and surname: Imre Keseru, VUB
    Address: Pleinlaan 2, 1050 Brussels
    Email contact: imre.keseru@vub.be
  - CLICKS and LINKS – for LOOPER collaborative / social platform
    Name and surname: Vin Sumner, Clicks and Links (CL)
    Address: Fourways House - 57 Hilton Street - Manchester M1 2EJ
    Email contact: vin.sumner@clicksandlinks.com

4.4. Obligations of LOOPER data controllers

IUAV, VUB, and MoU, as data controllers of the LLLs and of the project, as well as Clicks and Links, under their respective responsibilities, come under the following obligations:

1. To explain clearly and plainly the purpose of the project and of the living lab, giving due time to assimilate notions, tailoring information so that all persons can understand;
2. To illustrate the structure of the LL clearly: duration, venues, what will happen;
3. To explain what categories of personal data of research participants is processed, and explain the purpose of the processing;
4. To clearly indicate the national legislation regulating the processing of the personal information.
   a) The Privacy Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, for Belgium, https://www.privacycommission.be/en/privacy-act
   b) The Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) for Italy, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248
   c) The Data Protection Act of 1998 for the UK, https://www.legislation.gov.uk/ukpga/1998/29/contents;
5. Not to share data collected during the research with third parties or outside the project.
6. This means that under no circumstances, location data or identification data can be shared with any organisation or entity outside the consortium LOOPER, without the consent of the participants;
7. To retain location data no longer than necessary.

8. The list of names of participants in the LL and the location data of participants must be deleted or rendered irreversibly anonymised, in any case, no later than 1 month after the end of the project.
9. To ensure participants can access the data concerning them at any time.

Research participants have a right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and where that is the case, access to the personal data. Upon receiving the request, the Looper partner will provide a reply to the data subject request, such as a copy of the data collected, no later than 15 days from first request.

4.5. Identification data of participants in physical meetings

The list of participants in LOOPER Living Labs contain name, surname, and an email address or a contact detail of the research participants.

The list is held by the project partner in charge of each living lab which acts as "Verona/Brussels/Manchester data controller" (see above).

This list should not be disclosed except for a purpose related to the project activities (e.g. during project meetings).

LOOPER data controllers are responsible for the secure storage of the list of names participating in the LOOOPER Living Labs, which must be kept in a secure place. The list must not be disclosed outside the LOOPER consortium and not published in deliverables. In any case, the list should not be made public, unless the disclosure is required by proven needs and legitimated purposes or interests that are recognised in the law. In deliverables of the project, the names of participants should be obfuscated so that they are identifiable.

During the LOOPER Living Labs, citizens are encouraged to freely express their opinions; these opinions cannot be disclosed by the data controller or by LOOPER partners in any form in forums different than the project's dedicated places, both online (web site, social media) and offline (reports, deliverables), without the consent of the person who has expressed them. Data controllers are responsible for living up to participants' reasonable expectation of privacy even when they participate in public debates.

4.6. Access logs and IP addresses of participants in online activities

Data Controller Clicks and Links is responsible for implementing a web site cookie policy ensuring that cookies are not being used to gather information unnecessarily.

Participant access log entries in the LOOPER collaborative platforms will be maintained, containing date, the time, the username. To prevent tampering, user access logs will be stored in a secure centralized server and will be kept for the duration of the project.

4.7. Location data of participants from participatory sensing and geotagging

Arguably, the processing activity that poses the highest risks to data subjects concerns the processing of data bout the location of citizens involved in "participatory sensing" and in "geotagging" the public realms.

When using Air Casting or Air Beam device, the individual must download an app and register using his or her name, a user name and e-mail address. http://aircasting.org The registered Air beam user is assigned a unique number. As he or she activates the device which records, e.g., data about air pollution, his or her location is traced. The participant must then upload the data into the Air casting Crowd Map. The data is subsequently retrieved by LOOPER partner IUAV stored and visualised in the LOOPER platform and web site.

Air Casting has a Privacy Policy, which states:

> AirCasting App Privacy Policy
>
> by Michael H

AirCasting is a HabitatMap project. HabitatMap is a non-profit environmental health justice organization whose goal is to raise awareness about the impact the environment has on human health. HabitatMap will never collect any personally identifiable information about you through the AirCasting app unless you have provided it to us voluntarily, nor will we use any information gleaned from your Android device to market to you or pass your information to any third party.

Location: To geolocate your measurements, the AirCasting app requests permission to access your location. The AirCasting app has several features that enable location data to remain private. AirCasters can "disable maps" in the app settings, which turns off GPS tracking. When AirCasters record data with the GPS disabled, the data never leaves the Android device and is never synced to our servers. AirCasters can elect to save their data to the AirCasting server but not contribute it to the "CrowdMap". This means the data can only be viewed on the website via a link that you generate inside the app when signed in. AirCasters can also elect to send the data from the app directly to their own server, entirely bypassing the AirCasting server. In addition, when recording fixed indoor sessions, GPS coordinates are never logged.

Source: http://www.takingspace.org/aircasting-app-privacy-policy/ (download 05.05.2018)

In the LOOPER context, the participant subject will be identifiable since his or her location is linked to his or her individual's name, e-mail address or a unique number. Linked location data may reveal a person's movements over a period of time, enabling for example to identify their home address or place of work based on their daily routine.

In addition, as part of geo tagging activities, participants may take pictures or recordings and upload them to the LOOPER online platform and map. In this case, the user consents that his or her location, when she or he took the picture, is recorded and his or her name is displayed in the map of the area object of the study, hosted in the LOOPER platform.

To mitigate the risks of locating a participant and determining, e.g., whether he or she is home or not, whether she or he is in a particular area, research participants are advised to use only their first name or a pseudonym.

Pseudonymisation is a technique that consists in replacing one attribute (typically the name) in a record, by another. Only a pseudonymous ID number is used to link individual-level data with participants' identities. However, given the nature and the scope of the project, which is based and encourages participation in the public realm, it may be important that participants use their real name and just the initial of the surname, in the ULL activities. Using their real time, they will develop a sense of the importance of the work they are doing, and of their active contribution to the public realm. When people use nick names or pseudonyms there is a risk that the quality of contributions be poorer.

However, participants must be made aware of the possibility to choose a pseudonym and must be told the reasons why the project prefers the use real names.

As a further mitigating strategy, participants should be able to upload the data gathered from participatory sensing directly into the LOOPER platform, without having to upload them in the Crowd map of Air Casting (see D2.1 Section3).

IUAV, VUB, UoM as the partner responsible for living labs are responsible for

- Training the participants in the use of the monitoring and tagging devices;
- Giving the participants the choice between pseudonym and real name and to obtain permission to use their real name in reporting monitoring and geotagging activities;
- Advise to turn off the device or add tags when at home or when entering places like hospitals, trade unions, associations as this info may be reveal sensitive information about them (unless the monitoring targets those specific areas).
- Store the retrieved data securely

See Annex II: information must be provided concerning the processing of location data to participants using location based or geotagging technologies.

4.8. Secured storage, transmission, and retention

Any personal data must be transmitted securely to the LOOPER platform, for instance by encrypting the data.

VUB is responsible for ensuring the secured transmission of personal data between project partners, if any.

Personal data of research participants cannot be stored for a period of time longer than what is necessary to attain the purpose of the processing activities. In any case, personal data of research participants should not be stored beyond one month after the end of the project or for further periods in accordance with the law.

4.9. Environmental Public available information

As mentioned earlier, publicly available information is not subject to data protection law. The EU directive on access to environmental information provides that individuals have the right to access environmental information held by public authorities.

This entails that the participants in the urban living labs have the right to request to and obtain from local, regional or national public authorities access to environmental information, including air quality and noise road safety / parking or public greenspaces, raw data, daily data, compiled data, reports, statistics, values monitoring in hazardous air pollutants, indexes…etc.

In addition to data, participants in Looper Living Labs LLL have the right to access measures, including administrative measures, such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect air, noise levels, road safety/parking or public greenspaces. For instance, citizens have a right to know how many trees are going to be planted as mitigating measures in a given area, what areas are dedicated to parking, etc.

Public authorities must provide the information requested within a month, save for the exceptions foreseen in the law, as mentioned earlier in section 3.2.

5. RECOMMENDATIONS TO LOOPER DATA CONTROLLERS

This table summarises the data protection implications for the LOOPER projects, offers recommendations to partners, and identify partners responsible for implementing the suggested measures.

Data protection research issue	Recommendation	Responsible partners
Participation in LLL is voluntary and based on informed consent	Inform potential participants and urban stakeholders via public channels, conference, meetings; inform them about purpose and the methodology of the project; explain that they can leave the lab at any time.	VUB and BRAL – BXL LA – VER UoM and - MAN
Obtain informed consent	Prepare and ask participants to sign a consent form (see Annex I and Annex II for a template)	VUB and BRAL – BXL LA – VER UoM and - MAN
Participatory sensing activities and geotagging using mobile geo-location devices	Participants must be informed and consent to this type of data collection, the method of collection and the use location data pertaining to them.	VUB– BXL IUAV – VER UoM – MAN
Identification data	Keep the list of names in a secured place and treat them confidentially	VUB– BXL IUAV – VER UoM - MAN
Retention of identification and location data	Data should not be kept longer than necessary to attain the project's purposes and deleted or anonymized one month after the end of the project.	VUB
Security measures		
Pseudonymisation of location data	Participants must be given the choice to use a pseudonym or their real name when location data is processed	VUB– BXL IUAV – VER UoM – MAN CLIKS and LINKS
Security measures	Turn off device when home and when entering places like hospitals associations, trade unions…	VUB and BRAL – BXL IUAV and LA – VER UoM and - MAN

Table 1. Recommendations to LOOPER data controllers

6. ACKNOWLEDGEMENTS

The support of Brussels Capital Region – Innoviris (Belgium), Ministero dell'Istruzione dell'Università e della Ricerca (MIUR) (Italy), the Economic and Social Research Council (UK) and the European Union is gratefully acknowledged.

7. REFERENCES

Article 29 Data Protection Working Party, Opinion 15/2011 of the Article 29 Data Protection Working Party on the definition of consent (WP187) 13 July 2011

Article 29 Data Protection Working Party, The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Adopted on 01 December 2009, 02356/09/EN, WP 168.

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European law journal, 13(4)*, 447-468.

Bygrave, L. A. (2000). *Data Protection Law. Approaching Its Rationale, Logic and Limits.* The Hague, London - New York: Kluwer Law International.

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.

Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and No. 14, Rome, 4 November 1950, ETS No. 5. http://conventions.coe.int/treaty/en/treaties/html/005.htm

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 181. http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47

Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995

European Commission. 2017. Position paper transmitted to EU27 on the Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date. TF50 (2017) 14 – Commission to EU 27

European Court of Justice (ECJ) C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González).

Goldman, J., Shilton, K., Burke, J., Estrin, D., Hansen, M., Ramanathan, N., ... & West, R. (2009). Participatory Sensing: A citizen-powered approach to illuminating the patterns that shape our world. *Foresight & Governance Project, White Paper*, 1-15.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016

ANNEX I - INFORMED CONSENT FORM FOR PARTICIPATION IN LOOPER LIVING LABS

"I, undersigned [name] [date and place of birth – natural person; registry number – legal entities] [contact details] [if representing a minor: her/his name, date of birth, etc.], hereby give my consent to take part in the research carried out by the LOOPER Research Consortium.

1. I have been informed that the LOOPER project is a research project currently run under the European Union ENSUF Framework under the grant agreement no. [number]. The co-ordinator of the project is the Vrije Universiteit Brussel (VUB, Brussels (BE).
2. I have been informed about the purposes of the project. I have had all my questions answered to my satisfaction.
3. My participation in the research will include participation in meetings and, if I agree, participatory sensing and online communication activities. Information obtained during the research will be used for advancing knowledge and tackling the problem of air pollution/ traffic/ anti-social behaviour. My personal data will be made available only to the members of the LOOPER Consortium.
4. I understand that no further use of my personal information in the course of the project is foreseen.
5. I understand I will not be paid for my participation.
6. I give this consent fully informed, freely and voluntarily and I understand that I am free to withdraw my consent and discontinue my participation at any time without any negative consequences.
7. The relevant laws of [country] shall apply.

Done in two copies, of which one is for the LOOPER Consortium and one for the participant.

Done at [place] on [date].

Signature"

ANNEX II - INFORMATION TO BE PROVIDED TO CITIZENS USING LOCATION BASED AND GEOTAGGING TOOLS

In addition to the information provided to participants, specific information must be provided concerning the processing of location data to participants using location based or geotagging technologies.

- Inform participants that the use of geotagging tools is voluntary and that he or she can withdraw at any time
- Inform LOOPER participants what happens if they chose to use geotagging tools
- Explain that geotagged content such as pictures and videos are uploaded on LOOPER and saved into an application server.
- Clearly explain that the geotagged content contains location information positioned by the mobile device.
- Inform about use of location information derived from mobile devices
- Inform about in which context, the project living lab and its aims, the disclosure of information takes place.
- Inform who is on the receiving end of the information flow, other participants, the partner organizations etc..
- Inform participants that they can choose a pseudonym and of the reasons why the project prefers the use of real names.
- Ask explicitly if the application may identify the location of the mobile device.