This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement n° 101037648 – SOCIO-BEE

SOCIO-BEE

Grant Agreement No: 101037648
[H2020-LC-GD-2020-3]

Wearables and droneS fOr CIty Socio-Environmental Observations and Behavioral ChangE

Deliverable

D1.6 - Data Management Plan.R2

Workpackage No.	**WP1**	Workpackage Title	**Project Management and Administration**
Task No.	**T1.3**	Task Title	**Data management**
Lead beneficiary		**VUB**	
Dissemination level		***PU***	
Nature of Deliverable		***ORDP***	
Delivery date		**31 May 2023**	
Status		**F**	
File Name:		**[SocioBee] D1.6 - Data Management Plan.R2_final.pdf**	
Project start date, duration		**01 October 2021, 36 Months**	

Authors List

Leading Author (Editor)			
Surname	*Initials*	*Beneficiary Name*	*Contact email*
Chomczyk Penedo	ACP	VUB	andres.chomczyk.penedo@vub.be
Fabcic Povse	DFP	VUB	danaja.fabcic.povse@vub.be
Quinn	PQ	VUB	paul.quinn@vub.be

Co-authors (in alphabetic order)				
#	*Surname*	*Initials*	*Beneficiary Name*	*Contact email*
1	N/A	N/A	N/A	N/A

Contributors (in alphabetic order)				
#	*Surname*	*Initials*	*Beneficiary Name*	*Contact email*
1	Kyfonidis	CK	CERTH	kyfonidis@iti.gr
2	Drosou	AD	CERTH	drosou@iti.gr
3	Jimenez Train	AJT	ZGZ	ajimenez@zaragoza.es
4	Garcia Zubia	JGZ	UDEUSTO	zubia@deusto.es
5	Ortiz-Coronado Lopez	MOCL	UDEUSTO	mortiz@deusto.es
6	Lopez de Ipiña	DLI	UDEUSTO	dipina@deusto.es
7	Watelet	EW	ID2M	emilien.watelet@id2move.eu
8	Morresi	NM	UNIVPM	n.morresi@pm.univpm.it
9	Revel	GMR	UNIVPM	g.m.revel@univpm.it
10	Casaccia	SC	UNIVPM	s.casaccia@staff.univpm.it
11	Udina	SU	BETTERAIR	sudina@bettaircities.com
12	Varga	DV	VUB	Dorottya.Varga@vub.be

Reviewers List

List of Reviewers (in alphabetic order)				
#	*Surname*	*Initials*	*Beneficiary Name*	*Contact email*
1	Kopsacheilis	EVK	CERTH	ekops@iti.gr
2	Sarcina	AS	UNIPD	andrea.sarcina@unipd.it
3	Amadei	CA	UNIPD	claudia.amadei@unipd.it

Document History			
Date	*Version*	*Author*	*Description*
13/03/2023	0.1	**ACP**	First revision and cleanup from previous 1st release
17/04/2023	0.2	**ACP**	Second revision with comments from partners
02/05/2023	0.3	**ACP**	Third revision with comments from partners
15/05/2023	0.4	**ACP**	Fourth revision with comments from partners
17/05/2023	0.5	**ACP**	Fifth revision with internal VUB comments
24/05/2023	0.6	**ACP**	Sixth revision with internal VUB review
31/05/2023	1.0	**ACP**	Final version for peer review
02/06/2023	1.1	**ACP**	Final version incorporating comments from peer review

List of definitions & abbreviations

Abbreviation	Description
CESSDA	Consortium of European Social Science Data Archives
CF	Consent Form
CS	Citizen Science
DMP	Data Management Plan
DPO	Data Protection Officer
DPP	Data Protection Policy
DSP	Data Security Protocol
D&W	Drones & Wearables
EC	European Commission
EAB	External Advisory Board
ECA	Ethics Committees Approvals
EEAB	External Ethics Advisory Board
ENISA	European Union Agency for Cybersecurity
EU	European Union
G.A.	Grant Agreement
GDPR	General Data Protection Regulation
GIS	Geographic Information System
GPLEM	Gender, Ethics, Law and Privacy Manager
N.A.	Not applicable
ORD Pilot	Open Research Data Pilot
PC	Project Coordinator
PII	Personally Identifiable Information
PM	Project Manager
PMR	Periodic Management Reports
REP	Research Ethics Protocol
SC	Steering Committee
TfIS & CF	Templates for Information Sheets

Executive Summary

The content of this deliverable is SOCIO-BEE's D1.6 - Data Management Plan (DMP), which is due in project month M20. The DMP is a living document, dependent on highly collaborative work and the input received by the consortium, and will be updated as the implementation of the project progresses and when significant changes occur. This is the second of three versions of the Data Management Plan within the framework of the SOCIO-BEE project.

This deliverable consists of **two** main parts. The first part includes an analysis of the main elements of the data management policy to be used concerning the project and therefore uses the Horizon 2020 FAIR DMP template, in line with the requirements of the Open Research Data Pilot of the European Commission, which has been designed to be applicable to any Horizon 2020 project that produces, collects or processes research data. Second, this deliverable is also part of the SOCIO-BEE's Ethics Commitments Strategy and is additionally used as a space for reporting on the partners' ethics commitments and progress as well as concerns and questions. The Ethics Management Plan describes the main procedures of the SOCIO-BEE project to operate based on ethics principles during all the research processes and during all the SOCIO-BEE project implementation. It aims to describe the fundamental ethical issues relevant to the project, as well as specific implications with respect to citizen science, and present all the procedures to be followed by the SOCIO-BEE consortium partners working in the project.

This second version of the DMP provides an updated overview of the project's data management policy and the Ethical Management Plan guidelines. It materializes the efforts of the partners with respect to their data and ethical management while designing their research approach. In addition, this document contains a detailed description of the various legal data protection and ethical requirements necessary for the project and implemented so far. Finally, several draft as well as adopted customizable templates have been provided in annex regarding legal and ethics requirements, with emphasis on personal data protection. It also includes the second iteration of the Research Ethics Protocol for SOCIO-BEE citizen scientists.

The next version of the SOCIO-BEE Data Management Plan (M36) will report on how the SOCIO-BEE consortium has efficiently managed its research data in terms of storage and backup, selection and preservation, as well as update the scope and description of datasets that will be made available. It will also become clearer to what extent the data in SOCIO-BEE is Findable, Accessible, Interoperable and Re-usable (FAIR). Updates regarding ethical concerns, guidance and templates as well as relevant legal developments will also be provided, once this information becomes available.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose of the document

Task T1.3 of the SOCIO-BEE Work Package 1 involved the development and delivery of the Data Management Plan (DMP, D1.5) as well as its updates (D1.6 and D1.7), which includes an analysis of the main elements of the data management policy (IEC 62.531) to be used concerning the project. VUB, in close cooperation with the Project Coordinator (PC), the Project Manager (PM) and the External Ethics Advisory Board (EEAB), coordinates the efforts to characterize the nature and the type of the data produced, providing support to other partners in the consortium and ensuring standardization of the data and availability in the most appropriate scientific repository (e.g., the European Open Science Cloud). The data must be searchable, accessible, interoperable, and reusable (FAIR). All partners are expected to provide their input. The DMP includes: (i) Reference and name of the data set as well as the organization in charge (including contact details); (ii) Description of the data set (origin, nature, utility, etc.); (iii) Standards and metadata; (iv) Data exchange (access procedures); (v) Archiving and preservation (long-term preservation procedures); (v) A list of the software tools envisaged to be used during the project for research purposes and justification (vi) The data security protocol (including organizational and technological measures); (vii) Brief overview of the data protection legal requirements, including the contacts of the partners' designated Data Protection Officers (DPO) or in case there is no designated DPO, the organization's data protection policy. The DMP was delivered in M6 with partial input from D3.1 and will evolve during the project (updates in month M20 and M36). This 2nd release presents those evolution developments that took place up to M20. The consortium is fully aware of the requirement of Open Access for scientific publications as set out in Article 29.2 of Grant Agreement H2020. All peer-reviewed publications arising from SOCIO-BEE will provide open access to scientific publications of the project (gold access in the first instance; green, as a contingency), without compromising the exploitability of the project results.

The Data Management Plan is also part of the SOCIO-BEE's Ethics Commitments Strategy and will be additionally used as a space for reporting on the partners' ethics commitments and progress as well as concerns and questions.

This is the second version of the DMP submitted in the twentieth month of the SOCIO-BEE project. The DMP will follow its first version delivered on the sixth month of the SOCIO-BEE project, which built upon the template provided by the European Commission (EC) and the conditions for the Open Research Data Pilot.[1] The latter refers to: a) the development of a plan and b) the provision of research data in open access, wherever possible, following the principle "as open as possible, as closed as necessary".

1.2 Relationship with other deliverables

D1.6 is closely related to D3.1, D3.2 and D6.1 and will govern the way SOCIO-BEE researchers make their research data available, using the best efforts to ensure open access as possible and in compliance with GDPR.

[1] European Commission, 'Guidelines on FAIR Data Management in Horizon 2020', 26 July 2016. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

1.3 Changes with D1.5

Considering that D1.6 is an update to D1.5, it builds extensively on it and improves on the following topics:

- further specification of the involved datasets (2.3.7);
- introduction of the BETTERAIR platform (2.6.3);
- update of the software tools involved in the project (2.9);
- execution of the joint controllership arrangement (2.10.6);
- preparation of the pilots' documentation (2.11);
- and incorporation of the relevant documents involved in the previously mentioned updates.

2 Data management plan (DMP)

2.1 The DMP Template

This deliverable uses the Horizon 2020 FAIR DMP template which has been designed to be applicable to any Horizon 2020 project that produces, collects, or processes research data.[2]

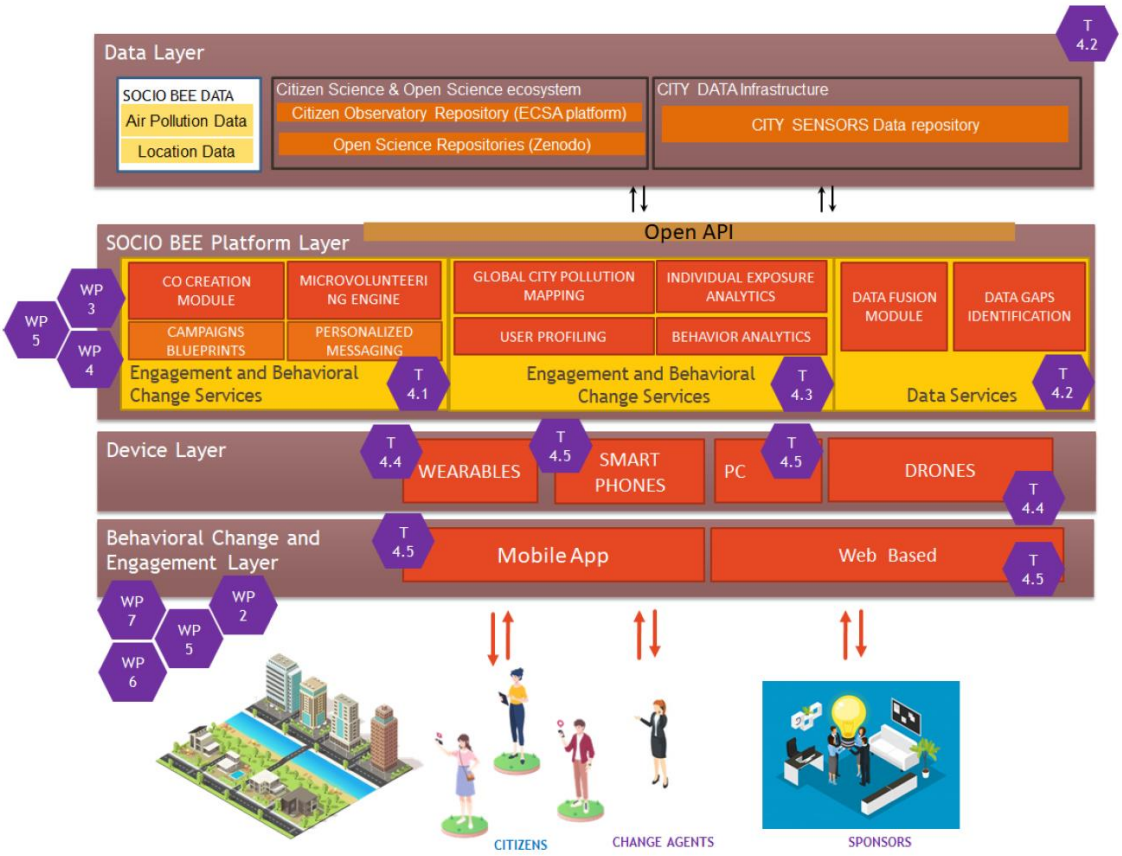

Figure 1. Initial architecture of the SOCIO-BEE platform

[2] Ibid.

2.2 The objectives of the project

The SOCIO-BEE platform aims to tackle present challenges in the field of citizen and open science by facilitating the participation of citizen scientists and the uptake of their research by key stakeholders. This allows citizens of all ages to take active part in their region's local decision making as well as better grasp what is at stake for the environment and through a participatory and inclusive approach to contribute to environmental policies development and improve considerably their daily life, in particular with respect to air quality. Moreover, it permits professional researchers, citizen researchers, local governments, and private entities to engage in a cycle of co-research and co-creation, towards the realization of SOCIO-BEE objectives.

2.3 Data summary

From the HORIZON 2020 FAIR DMP template, five crucial questions are asked that are needed to compile the data in the SOCIO-BEE project. These five questions are discussed in more detail below. Subsequently, these questions were also put to different partners in SOCIO-BEE in order to get an initial overview of the possible data in the project.

2.3.1 Purpose of data collection/generation and its relation to the objectives of SOCIO-BEE

The purpose of collection and generation of data throughout the SOCIO-BEE project is to achieve the main goal and strategic objectives of the project. Specifically, the data collected from the sources described below is used:

a) to develop a citizen science-based web platform to allow CS Hives in the active collection of environmental and socio-economic data through wearable technologies, sensors, apps and research-based instruments;
b) to conduct research on the collected data to enable insights;
c) to manage and disseminate information about the SOCIO-BEE related research and exploit its results.

The data layer of SOCIO-BEE is dedicated for storing and retrieving the data that is utilized by the SOCIO-BEE platform, including data from citizen science, European open science and city data infrastructure. Technically speaking, SOCIO-BEE will be built on existing private data, new data collections via apps, sensors, surveys and launched open data initiatives to provide broad access to environmental data from the public sector and at the same time support scientific research and the development of new business opportunities. The interconnection with 13 external data sources will promote knowledge evolution derived from 'big environmental data' (generated at different scales) with particular focus on urban health. Moreover, collection and generation of data are necessary to manage the project, disseminate the information about it, analyze and exploit its results.

2.3.2 Types of data

The data collected and processed in the SOCIO-BEE project can be divided initially into two categories:

- Non-personal data: any data that do not fall into the scope of the General Data Protection Regulation (GDPR);
    - Experimentation & testing Mock-up data
    - Air pollution data from existing networks of static air quality measuring deployed in the cities

- Experimental air quality data acquired by the citizens using WSNs
- GIS-data

- Personal data: under article 4 of the GDPR the personal data is defined as any information relating to an identified or identifiable natural person (data subject). In turn, the 'identifiable natural person' is "anyone 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 (e.g. IP addresses) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
  - Types of personal data:
    - The current scope of the possible personal data used is as follows. with respect to research participants:[3]
      - full name
      - date of birth
      - citizenship
      - gender
      - education background
      - professional background
      - other socio-economic information
      - data concerning health or disability (only if necessary for safety purposes or for allowing the adoption of accessibility measures to facilitate participation)
      - IP-addresses
      - image or video of the research participants
      - voice of the research participants
      - textual data from research participants
      - behavioural elements concerning
        - interaction with the city and the environment (use of public transport, exercise, etc.)
        - attitudes and motivation

It is important to keep in mind that it will not be always easy to differentiate between datasets with personal and non-personal data. If that is the case, then the datasets will be considered mixed and will fall under the framework for the processing of personal data. The processing of non-personal data is governed by Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union.[4]

The personal data will be collected and processed within the project under the current EU regulations and respective implementing national legislation that is described in more details in the next sections of this deliverable and have already been touched upon in D3.1 (M04). Specifically, the General Data Protection Regulation and the respective national legislation.

[3] See Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648, p. 77
[4] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303, 28.11.2018, p. 59–68*

While the SOCIO-BEE consortium did not foresee the processing of special categories of personal data when drafting D1.5, except for safety, inclusion and accessibility purposes, it has been deemed necessary to process certain categories pertaining to gender. As processing of special categories of personal data is in principle prohibited, this has been addressed via the collection of the participants' consent; more on this in section 2.11. Special categories of personal data include:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

The processing of special categories of personal data can only occur exceptionally under special exemptions, which however, must be interpreted strictly and narrowly. In the case of SOCIO-BEE, if processing of special category data is necessary at any stage, this will take place in line with Article 9(2)(a) GDPR. In other words, the data subject must have given explicit consent to the processing of those personal data for one or more specified purposes (except if Union or Member State law prohibits this exemption). Explicit consent must be also documented and a proof must be kept, usually in written form. Again, in the case of public authorities, it may be necessary to consider processing for public interest purposes. Vulnerable data subjects may include as well, apart from children, other adult individuals belonging to a population group which requires special protection, for instance elderly persons or persons with disabilities. In that case, the SOCIO BEE partners will identify and implement specific safeguards, including the conduct of a Data Protection Impact Assessment (in WP6), as part of its overall Impact Assessment and the full implementation of the principles of Data Protection by Design and by Default.

2.3.3 Re-using of existing data

The project will use already existing information from:

- Municipalities:
    - SOCIO-BEE will leverage from the existing networks of static air quality measuring deployed in the cities of Zaragoza, Ancona and Maroussi
    - The project will also leverage from their Open Data portals and the air quality agencies of the regions where they are located.
        - Ancona
            - City pollution data
                - Data collected by the smart urban pollution sensors (ARPAM)
        - Amaroussion
            - City pollution data
        - Zaragoza
            - City pollution data

- Air pollution monitoring network provided by Zaragoza City Hall (datosabiertos.zaragoza.es and https://www.zaragoza.es/sede/portal/medioambiente/calidad-aire/datos/servicio/calidad-aire/)

2.3.4 Origin of the data

At this stage, the SOCIO-BEE has identified its data sources in the table below:

Table 1. Data sources SOCIO-BEE

PData sources			
Purpose	**Source (tool)**	**Source (actor)**	**Potential Data**
Creation of the citizen-science web platform	wearables drones and sensors	citizen scientists	Air pollution data; Location data
Research conducted based on data collected by citizen scientitists	wearables drones and sensors	SOCIO-BEE researchers	Air pollution data; Location data
Dissemination and communication activities	Sign up, consent forms, social media, website	SOCIO-BEE researchers	sign up and consent forms may include name, signature, contact details
• To assess pilot participants' feedback, SOCIO-BEE will use surveys to determine citizens' perception of the SOCIO-BEE tools within their specific pilot contexts • For the extraction of user requirements and the organisation of activities; • to evaluate personal change of citizen scientists during the project; • profiling users, using surveys to identify peolple within a community with the potential to be a queen bee	Questionnaires and surveys; Online, maybe through a mobile phone embedded in an app or through an external source such as Survey123, Google Forms, Survey Monkey or a own developed framework	Citizen scientists	Demographic data, data relating to attitude and motivation towards the cause and behaviours that can be relevant for citizen science
To understand the underlying barriers, drivers and motivations to become a citizen scientist or an ambassador for behavioral change, and understand their communication preferences (e.g., need for cognition)	Focus group discussions and in-depth interviews as well as survey information (Prolific)	Citizen scientists	data relating to attitude and motivation towards the cause and behaviours that can be relevant for citizen science
Existing datasets needed to complement dynamic citizen science data for more insights	City data infrastructure	Municipalities: Ancona, Amarousio and Zaragoza	Air pollution data
• Data gap identification • Methods developed will facilitate the performance of what-if analyses and hypothesis testing • Make analysis for individual exposure to pollution and an overall spatial pollution	wearables drones and sensors	SOCIO-BEE researchers; Citizen scientists	• Sensor-collected data as time series • Images collected by drones • Textual data from Users • GIS data • City pollution historic/live data

			• Individual exposure historic/live data • Behavior analysis of the SOCIO-BEE's users • Historic/live data from the wearable sensors • Historic/live data from external sources • Historic/live data retrieved from drones
Present personal exposure and footprint as long as analyse issues	Smartphones, cloud-platforms	SOCIO-BEE researchers	• WiFi connection • Experimental activity/Local Stored Data • Cloud Storage
Testing of SOCIO-BEE enablers (tools and components): Data collection infrastructure, AcadeMe	Mock-up data	SOCIO-BEE researchers	*N.A.*

2.3.5 Data size

At this point in the project, it is not yet clear what the expected sizes of the data will be. However, this is monitored and more information will be provided.

2.3.6 Data utility

The data generated in SOCIO-BEE might be useful to:

- SOCIO-BEE consortium;
- European Commission services and European Agencies
- The general public including the broader scientific community
- Businesses
- (Environmental) action groups
- (Local) decision-makers

2.3.7 SOCIO-BEE project datasets

Below the reader can find a second iteration of the SOCIO-BEE project datasets. **The template used to collect the information about the datasets can be found in Annex I**. This list will be updated in the next editions of D1.7 and the information will be further curated while new datasets may be included based on the progress of the architecture.

2.3.7.1 Dataset 1: Data Collected during the social media campaign

Fact sheet Dataset 1	
Dataset name	- Social Media Insights
Dataset description	- Text, Metadata and Images

General security and privacy considerations	- Anonymization/Pseudonymization
Datatype specific answers	
Datatype name	- String, Integer for Text and Metadata, and Images
Data description	- Text such as Posts in social media - Metadata such as number of reposts, likes etc. - 3-d double arrays for RGB Images
Data provider and reference	- CERTH - M12 (during the work done for Task 4.1)
Purpose of data collection	- User Classification - Will be Processed to Classify a User in SOCIO –BEE's classes
Relation to the project	- WP4, Task 4.1
Standards and metadata	- CSV
Data sharing and access	- Initially accessible from all SOCIO-BEE partners - Depending on data sensitivity, access will be limited
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server - - BETTAIR: storage and delivery of calibrated data

2.3.7.2 Dataset 2: SOCIO-BEE database (SOCIO-BEE devices and gathered data)

Fact sheet Dataset 2	
Dataset name	- SOCIO-BEE dataset
Dataset description	- Information collected by sensors, drones and mobile devices
General security and privacy considerations	- Gathered data, Confidential - SOCIO-BEE data, Public
Datatype specific answers	
Datatype name	- Multiple data-types (sensors, images from drones, textual data, spatial data)
Data description	- Sensor-collected data as time series - Images collected by drones - Textual data from Users - GIS data

Data provider and reference	- CERTH, BETTAIR - M12 (during the work done for Task 4.2)
Purpose of data collection	- Data gap identification - Methods developed will facilitate the performance of what-if analyses and hypothesis testing
Relation to the project	- WP4, Task 4.2
Standards and metadata	- CSV
Data sharing and access	- , CERTH, UDEUSTO, BETTAIR, IBER, ZGZ, MRSI, NILU, HOPU
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server - BETTAIR provides and stores calibrated data

2.3.7.3 Dataset 3: Data analytics

Fact sheet Dataset 3	
Dataset name	- History Dataset
Dataset description	- Date and Spatial
General security and privacy considerations	- Confidential Data
Datatype specific answers	
Datatype name	- Date datatype and Double datatype
Data description	- City pollution historic/live data - Individual exposure historic/live data - Behavior analysis of the SOCIO-BEE's users - Historic/live data from the wearable sensors - Historic/live data from external sources - Historic/live data retrieved from drones
Data provider and reference	- CERTH, BETTAIR - M13 (during the work done for Task 4.3)
Purpose of data collection	- Make analysis for individual exposure to pollution and an overall spatial pollution
Relation to the project	- WP4, Task 4.3
Standards and metadata	- CSV

Data sharing and access	- CERTH access
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server

2.3.7.4 Dataset 4: Mobile application data

Fact sheet Dataset 4	
Dataset name	- Activity
Dataset description	- General information provided by user's interaction with the device/ Credentials
General security and privacy considerations	- General Information, Confidential - Credentials, Encrypted
Datatype specific answers	
Datatype name	- Multiple data
Data description	- WiFi connection - Experimental activity/Local Stored Data - Cloud Storage - Collect data from sensors under request
Data provider and reference	- CERTH, BETTAIR, AUTH - M14 (during the work done for Task 4.5) - BETTAIR provides and stores calibrated data
Purpose of data collection	- Present personal exposure and footprint as long as they analyze issues
Relation to the project	- WP4, Task 4.5
Standards and metadata	- CSV
Data sharing and access	- CERTH, BETTAIR, AUTH - No access on Credentials
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server

2.3.7.5 Dataset 5: Experimentation & Testing Mock-up data

Fact sheet Dataset 5	
Dataset name	- Experimentation & Testing Mock-up data

Dataset description	- Text, Numerical values and Metadata
General security and privacy considerations	- Anonymization / pseudonymization - Since this are non-real-life data, artificially created for testing purposes there is no privacy consideration and no related security measure to be employed
Datatype specific answers	
Datatype name	- String, Integer
Data description	- Text, numerical data created as mock-up data simulating actual data from sensors, drones, or smartphones - The mock-up data may represent statistical values, outliers, insights etc. formed via the processing of a data distribution with specific properties - Metadata generated as mock-up data as a result of data generation algorithms taking a distribution with specific properties as input
Data provider and reference	- SOCIO-BEE partners of WP4 (starting from M7)
Purpose of data collection	- Testing of SOCIO-BEE enablers (tools and components): Data collection infrastructure, AcadeMe
Relation to the project	- WP4 / T4.2 / Data collection connection, harmonization, processing, orchestration and metadata - WP4 / T4.5 / SOCIO-BEE AcadeMe: web and mobile front-ends development
Standards and metadata	- CSV
Data sharing and access	- Access will be granted by HYP (access control for selected subsets) to: o Members of the HYP working team for SOCIO-BEE o Partners of WP4 (CERTH, BETTAIR, IBER, ZGZ, MRSI, NILU, HOPU) o Dissemination of interesting insights generated through processing of actual data
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server - Copy at a dedicated server at HYP premises

2.3.7.6 Dataset 6: Role definition and assignment in SOCIO-BEE

Fact sheet Dataset 6	
Dataset name	- Role definition and assignment in SOCIO-BEE

Dataset description	- Through different online questionnaires we will understand what the main traits of the participants in SOCIO-BEE project are to link them with the main bee roles in the project. The questionnaire/tool will not record any socio-demographic or socio-cultural information as we understand that anyone can become whichever bee-role irrespective of their gender, income, age, etc.
General security and privacy considerations	- Anonymization / pseudonymization will be always ensured but we do not plan to ask any personal information that can link the information collected to the specific participant in the SOCIO-BEE campaigns.
Datatype specific answers	
Datatype name	- Likert scale or scoring/ranging questions.
Data description	- We will use validated tools, mainly surveys, to understand participants' ○ Environmental knowledge ○ Environmental Values ○ Emotional involvement ○ Environmental Attitudes ○ Skills ○ Practices and Habits ○ Perception of Self/Collective-Efficacy ○ Social and cultural drivers ○ Institutional factors as a barrier ○ Economic factors (access to external budget)
Data provider and reference	- UDEUSTO university ○ Researchers from UDEUSTO will create the tool for gathering the aforementioned information and link them to the different roles in the project.
Purpose of data collection	- Better understand the different roles we will have in the Hive to better assign tasks or offer them tailored information. - We do not aim to understand who is behind a role, only know what the traits of a participant are to provide her bespoke information
Relation to the project	- Mainly WP2 for designing tailored engaging strategies and to WP4 when designing and implementing the recommendation engine and the micro-tasks.
Standards and metadata	- MS Excel file spreadsheets.
Data sharing and access	- WP2 people, WP4 colleagues always Anonymized ○ Within partner's facility
Data archiving and preservation	- In institutional Google Drive of the University of UDEUSTO.

	- In a shared database of SOCIO-BEE in which people may access to the role (not to the traits) by using a API call or similar way to extract this information. Still to decide

2.3.7.7 Dataset 7: Air Quality Data

Fact sheet Dataset 8	
Dataset name	- Multivariate, Time-Series (Numerical), String
Dataset description	- City pollution and weather measurements:
General security and privacy considerations	- Public research dataset
Datatype specific answers	
Datatype name	- String, Integer, Float
Data description	○ Year, Month and Day of the measurement. ○ PM2.5, PM10, SO2, NO2, CO, O3 concertation measurements ○ Temperature, Pressure, Dew point temperature, RAIN, Precipitation, Wind direction measurements ○ Monitoring site name
Data provider and reference	- UCI Machine Learning Repository (Beijing Municipal Environmental Monitoring Center)
Purpose of data collection	- Development and Evaluation of the AI models.
Relation to the project	- WP4 / T4.2, T4.3
Standards and metadata	- CSV
Data sharing and access	- Public access
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server

2.3.7.8 Dataset 8: Satellite and Air Quality Dataset

Fact sheet Dataset 8	
Dataset name	- Satellite Images (Optical, Hyperspectral), Multivariate, Time-Series (Numerical), String

Dataset description	- Satellite images and city pollution and weather measurements:
General security and privacy considerations	- Public research dataset
Datatype specific answers	
Datatype name	- Arrays, String, Integer, Float
Data description	○ Air Quality station. ○ NO2 concertation measurements ○ Sentinel 2 data. ○ Sentinel 5P data
Data provider and reference	- Artificial Intelligence & Machine Learning (AIML) @ University of St. Gallen (zenodo)
Purpose of data collection	- Development and Evaluation of the AI models.
Relation to the project	- WP4 / T4.2, T4.3
Standards and metadata	- Npy, netcdf, CSV
Data sharing and access	- Public access
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server

2.3.7.9 Dataset 9: PM2.5 concertation dataset

Fact sheet Dataset 9	
Dataset name	- KnowAir
Dataset description	- Air pollution and weather data from 184 monitoring sites.
General security and privacy considerations	- Public research dataset
Datatype specific answers	
Datatype name	- Arrays, String, Integer, Float
Data description	○ Planetary Boundary Layer (PBL) height. ○ PM2.5 concertation measurements ○ u-component of wind. ○ v-component of wind ○ 2m Temperature

	○ Relative humidity ○ Total precipitation ○ Surface pressure
Data provider and reference	- https://github.com/shuowang-ai/PM2.5-GNN
Purpose of data collection	- Development and Evaluation of the AI models.
Relation to the project	- WP4 / T4.2, T4.3
Standards and metadata	- Npy
Data sharing and access	- Public access
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server

2.3.7.10 Dataset 10: Air Quality Data retrieved from Copernicus Atmosphere Monitoring Service (CAMS)

Fact sheet Dataset 9	
Dataset name	- CAMS
Dataset description	- Air Quality measurements for multiple stations collected from CAMS.
General security and privacy considerations	- Public real data
Datatype specific answers	
Datatype name	- String, Integer, Float
Data description	○ Date ○ PM2.5 concertation measurements ○ NO2 concertation measurements. ○ O3 concertation measurements ○ PM10 concertation measurements ○ Monitoring station lat, long
Data provider and reference	- Copernicus Atmosphere Monitoring Service (CAMS)
Purpose of data collection	- Development and Evaluation of the AI models.
Relation to the project	- WP4 / T4.2, T4.3

Standards and metadata	- Npy
Data sharing and access	- Public access
Data archiving and preservation	- CERTH based SOCIO-BEE dedicated server

2.4 FAIR data

The European Commission supports FAIR data as a framework to follow when designing a Data Management Plan. It has produced the 'Guidelines on FAIR Data Management in Horizon 2020' which guides Horizon 2020 beneficiaries to make their research data *Findable*, *Accessible*, *Interoperable* and *Re-usable* (FAIR).[5] This is a required concept (so-called FAIR data principle) by EU-Projects. It should support the exchange of scientific data and lead to knowledge discovery and innovation.
The FAIR data approach is described as seen in the Table below.

Table 2. FAIR approach

Findable data	Clear naming and versioning of (meta-) data, use of search keywords and DOI
Accessible data	Specification of how data are made available and what tools are needed to access data
Interoperable data	Use of standards and vocabularies for (meta-)data and datatypes
Reusable data	Specification of when - and for which duration - data are made available, licensing of data

2.4.1 Making data findable, including provisions for metadata

First, a fixed naming and versioning convention is necessary to make the data generated by the SOCIO-BEE project Findable (FAIR). Consistent naming and versioning conventions will boost the data searchability so that interested parties such as partners and stakeholders can discover the dataset they are interested in in an easy way.

2.4.1.1 Naming conventions used

For facilitating common browsing and storage in different platforms and OS's, no spaces should be used in the document names, and instead the dash character "-" should be used.

Project document names must start with the prefix "SocioBee" in order to facilitate quick identification and indexing. In particular, the following conventions are mandatory for certain types of documents.

Deliverable: **"[SOCIO-BEE] Dw.n-title.vX.Y.ext"**

Where

- "Dw.n[.m]" is the deliverable number
  - "w" is the WP number

[5] European Commission, 'Guidelines on FAIR Data Management in Horizon 2020,' [Online]. Available: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

- "n" is the numbering within the specific WP
- "vX.Y" is the version number
  - "X" is the version
  - "Y" is the sub-version
- "ext" is the file extension pertaining to the format used

For instance, the name of (the final version of) deliverable D8.1 sent to the EC is "[SOCIO-BEE]- D8.1-Communications and dissemination plan and activities -1st release.v1.0.pdf"

Technical Reports: **"[SOCIO-BEE] TR-title.vX.Y.pdf"**

Where:

- "vX.Y" is the version number
  - "X" is the version
  - "Y" is the sub-version

2.4.1.2 Approach for clear versioning

Deliverable and technical reports will have a version and subversion number e.g. for version 1.1 = "v.1.1".

2.4.1.3 Best practices

Different scientific disciplines have already put certain standards in place, please refer to the **DCC catalogue**, the **RDA Metadata Directory** or **FAIRsharing** for examples. These catalogues also offer information on more generic standards, such as **Dublin Core**, **DataCite metadata schema** or **CERIF**.

2.4.2 Making data openly accessible

2.4.2.1 Open access to publications

The consortium is fully aware of the requirement of Open Access for scientific publications as set out in Article 29.2 of Grant Agreement H2020. SOCIO-BEE will provide open access to research through "green" and "gold" models. Within the "green" model, authors will archive their papers in an online repository before, with, or after their publication. The access to the manuscripts will be provided directly by their authors. This self-archiving will be managed through different channels: through the project website, through partners' own websites, and through public repositories such as arXiv. Within the "gold" model, manuscripts will be provided in an open access mode as published, where publication costs will be covered by authors and access to the articles will be provided by publishers. Further details will be set in the dissemination plan detailed at the start of the project [T8.1].[6]

[6] Ibid., p. 42

2.4.2.2 Open access to research data

2.4.2.2.1 Open Research Data Pilot (ORD Pilot)

This deliverable (D1.5) is an Open Research Data pilot, which means the following as described in the H2020 Progamme – guidelines[7]:

1. [Projects] must deposit the research data, preferably in a research data repository. These are online research data archives, which may be subject-based/thematic, institutional or centralized. Useful listings of repositories include the Registry of Research Data Repositories and Databib. The Open Access Infrastructure for Research in Europe (OpenAIRE) provides additional information and support on linking publications to underlying research data. Some repositories like Zenodo (an OpenAIRE and CERN collaboration), allows researchers to deposit both publications and data, while providing tools to link them. Zenodo and some other repositories as well as many academic publishers also facilitate linking publications and underlying data through persistent identifiers and data citations.
2. As far as possible, projects must then take measures to enable third parties to access, mine, exploit, reproduce and disseminate (free of charge for any user) this research data. One straightforward and effective way of doing this is to attach Creative Commons Licenses (CC BY or CC0) to the data deposited. The EUDAT B2SHARE tool includes a built-in license wizard that facilitates the selection of an adequate license for research data.

At the same time, projects should provide information via the chosen repository about the tools available to the beneficiaries that are needed to validate the results, e.g. specialized software or software code, algorithms and analysis protocols. Where possible, they should provide these instruments themselves.

2.4.2.2.2 Anonymization techniques

"To ensure that data subjects cannot be identified in any documents (reports, publications) or datasets within the project, only anonymized and aggregated data will be made public. The responsible partner (the partner that is gathering the data) will follow all required anonymization procedures to make sure that the data subject is no longer identifiable. Consequently, during the process of anonymization, data identifiers need to be removed, generalized, aggregated, or distorted and a small cell analysis should be carried out by the responsible partner. At this point, it would be important to underline that anonymization is different than pseudonymization (GDPR treats it as a distinct category, see Recital 26). Anonymization is the process of encrypting removing personally identifiable information from data sets so that the people whom the data relate to remain permanently anonymous, and thus un-identifiable; whereas pseudonymization, as defined in the GDPR (which incentivizes its use in Recital 29,e.g.)., means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[8] Below we add a table containing a list

[7] European Commission, 'H2020 Programme – Guidelines to the Rules n Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020', [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf
[8] GDPR, Art. 4(5)

of good practices for anonymization of quantitative and qualitative data, using the tour guide on data management of the Consortium of European Social Science Data Archives (CESSDA) as source. [9] [10]

Table 3. Good practices for anonymization of data

Type of data	Good practices
Quantitative data	• Removing or aggregate variables or reduce the precision or detailed textual meaning of a variable; • Aggregate or reduce the precision of a variable such as age or place of residence. As a general rule, report the lowest level of geo-referencing that will not potentially breach respondent confidentiality; • Generalize the meaning of a detailed text variable by replacing potentially disclosive free-text responses with more general text; • Restrict the upper or lower ranges of a continuous variable to hide outliers if the values for certain individuals are unusual or atypical within the wider group researched.
Qualitative data	• Use pseudonyms or generic descriptors to edit identifying information, rather than blanking-out that information; • Plan anonymization at the time of transcription or initial write-up, (longitudinal studies may be an exception if relationships between waves of interviews need special attention for harmonized editing); • Use pseudonyms or replacements that are consistent within the research team and throughout the project. For example, using the same pseudonyms in publications and follow-up research; • Use 'search and replace' techniques carefully so that unintended changes are not made, and misspelt words are not missed; • Identify replacements in text clearly, for example with [brackets] or using XML tags such as <seg>word to be anonymized</seg>; • Create an anonymization log (also known as a de-anonymization key) of all replacements, aggregations or removals made and store such a log securely and separately from the anonymised data files.

2.4.2.3 How will the data be made accessible?

2.4.2.3.1 Repository information and documents

The exchange and archiving of information and documents (presentations, reports, deliverables, etc.) among the SOCIO-BEE consortium will be facilitated through the project's repository. The SOCIO-BEE repository is based on the NextCloud platform.

The access to the SOCIO-BEE-related data is ensured within the consortium via Nextcloud. The servers on which Nextcloud is hosted are administered by CERTH. "It provides access to data through a web interface and also a platform to view, sync and share the files across devices easily — all under user's control. It uses an open architecture, extensible via API for applications and plugins and it works with any storage".[11]

[9] CESSDA, [Online]. Available: https://www.cessda.eu/Training/Training-Resources/Library/Data-Management-Expert-Guide/5.-Protect/Anonymisation
[10] See: PROTEIN: D9.1 – Data Management Plan, CO.
[11] See: HBM4EU: D10.1 – Data Management Plan, [Online]. Available: https://www.hbm4eu.eu/wp-content/uploads/2017/08/Deliverable-10.1-Data-Management-Plan-August-2017.pdf

The use of the repository is restricted to the team members of each project partner, who can access it using credentials provided to them. The SOCIO-BEE repository is structured along the WP structure of the project, whereas additional directories refer to "Project Management" documents (e.g. where the final submitted versions of deliverables, PMRs etc. are stored), "Project Meetings" documents (where e.g. meetings presentations are stored) and "Dissemination Material".[12]

Access to data from outside the consortium will be decided at a later stage of the project, taking into account particular needs and restrictions.

2.4.2.4 What methods or software tools are needed to access the data?

Data will be published using standard file formats (txt, pdf, csv etc.). All data will be accessed using standard tools.

2.4.2.5 Where will the data and associated metadata, documentation and code be deposited?

Depending on the type of data (sensitive or not), it can be stored in different locations. For example, non-sensitive can be archived externally in a trustworthy open data repository. In contrast, highly confidential research data is to be archived in secured repository and only shared if approved by the relevant instance (DPO, TTO, Data Stewards etc.).

The first version of Deliverable 4.3 - Data Services for collection connection, harmonization, processing and annotation describes the services developed for the collection, processing and fusion of data, along with the description of the data gaps identification module and all modules developed within Task 4.2, as well as **the data storage mechanism.**

Data archiving and preservation will take place in, among other places:

- CERTH based SOCIO-BEE dedicated server

2.4.3 Making data interoperable

Depending on the data set in SOCIO-BEE it will or will not be shared with multiple partners who can use these data for SOCIO-BEE related research. For some data the access will be protected with encryption and thus login details will be required, for instance non-anonymized personal data.

A basic functional open source release of SOCIO BEE platform will be released in GitHub and/or at https://eu-citizen.science/ under an open source license. Basic versions of modules will be open sourced. Value added services will be licensed for commercial use by partners owning them. GitHub will be used for the storage of the software components that will be produced during the project and the GitHub repository will be used for code releases. Github is a web-based hosting service for version control, primarily for software source code. It also includes features such as distributed version control and source code management, access control, task management, and bug tracking. Access to Github projects is achieved via the standard Git command-line interface and all of the standard Git commands are supported. Github repositories are also available for registered and non-registered users to browse.

[12] See: SOCIO-BEE: D1.4 – Project Handbook, v1.0, p. 35

2.4.4 Increase data re-use (through clarifying licenses)

One of the objectives of SOCIO-BEE is to create an open and sustainable data analysis platform for the overall CS process: cross-referencing environmental data in cooperation with citizens, scientists, citizen observatories and local decision-makers. To interpret vast amounts of data, it is necessary to provide action groups with easy to use and intuitive tools which will allow them to make better actions for improving air quality in the cities. These tools must be able to curate, process and visualize information from various sources, and convert it into value-added information to democratize environmental citizens' action while improving new or existing interventions. One of these tools is a collaborative platform in which experts (e.g. scientists, air quality managers) assist group leaders in the understanding of gathered data. Therefore, there will be at least one open science repository in Zenodo per pilot connected with SOCIO-BEE platform.

In line with the research ethics and the principles of fair and transparent data processing, should SOCIO-BEE researchers consider to render the datasets available for future research, they should obtain the additional, explicit consent of the data subjects (and their legal guardians) to the secondary use of the data. Data subjects must be explicitly given the opportunity to opt out from such further processing.

2.5 Allocation of resources

2.5.1 What are the costs for making data FAIR in your project?

Setting up a Github-project does not produce any costs. The publishing of the basic functional open source release of SOCIO BEE platform is therefore ensured.

For internal project communication and data sharing, the NextCloud solution has been set up, as seen earlier. NextCloud is an open source product as well. Even though the software is free of charge, costs are generated by the two servers used.

The fact that both current repositories are based on open source software, ensure further transparency and prevent vendor lock-in.

2.5.2 Person/team responsible for data management and quality assurance

All consortium partners are expected to assure data quality and follow up on data management issues internally in their organizations and in the context of the project activities. For example, for the data collected by users and sensors, automated filters on the background will either insert the collected data into the database or flag them for further quality investigation. The Project Coordinator and the Steering Committee are in charge of quality assurance. VUB will oversee data management activities from the legal and ethical perspective via the updates of the Data Management Plan.

2.6 Data security

2.6.1 Datasets

State-of-the-art technologies will be used in the project to ensure confidentiality and security of the data included in datasets, such as encryption and authentication. With respect to the personal data the anonymization and pseudonymization techniques will be used (for example, the identifiers will be deleted, when possible, or stored separately from the other data). Whenever possible technically, these

techniques will be favoured and used in the storing of personal data for SOCIO-BEE. The technical details needed for the development of this technique in the project are not available and will be developed in WP3 as soon as the architecture for the project is defined.

In the event of personal data breach, the project partners will notify without delay their competent national supervisory authorities as well as the data subject(s) that may be affected by the breach, depending on a respective breach and risk assessment. At the same time, they will document the personal data breach in detail and all related information.

The SOCIO-BEE platform development puts particular emphasis on the principles of privacy/data protection by design and privacy/data protection by default.[13] This means that the relevant software and hardware will be designed and developed from the ground up in such a way that relevant data protection measures are taken into account from the outset. The technology design is oriented in all areas to the data protection requirements. The basic idea is that data protection can be most easily complied with if it is already fully technically integrated, to prevent unlawfully collected data (legal information provided in D3.1).

2.6.2 NextCloud

The Nextcloud solution is open source and has been audited by the NCC Group. The review against the control Clause 14 of ISO27001 'Security in Development and Support processes' was done in 2016 and can be downloaded from the NextCloud site (https://nextcloud.com/secure/). Since NextCloud is an on-premise service, NextCloud GmbH has at no time access to the data stored on the server. NextCloud also provides event logging, backup tools, fine-grained access control to files via groups, and the secure sharing of links by using passwords and expiration dates. NextCloud uses industry-standard SSL/TLS encryption for data in transfer.

2.6.3 BETTAIR platform

BETTERAIR stores air quality data and provides corresponding calibrated data with its state-of-the-art sensor modeling. All data is kept in BETTAIR's vault which is administrated entirely by BETTAIR, and is made accessible through an API that requires authentication and features all necessary security precautions for unauthorized data access.

2.7 Ethical aspects with respect to the data management

Some ethical and legal aspects, including the legal frameworks and the ethical procedures that, at both European and national level, researchers will comply with and take into consideration when processing personal data of research participants have been discussed in WP3 (D3.1) and will be regularly overseen in WP6 and in the Ethical Management Plan of D1.5. In D3.1, the ethical and legal implications were raised for both the practice of citizen science and for cutting-edge technologies in SOCIO-BEE such as drones, wearables and AI. For WP2 'Engagement, Behavioural Change and Pro-Environmental Stewardship', several online workshops on specific topics are organized with the aim of creating a shared understanding within the project and finding common solutions. Two of these workshops already dealt with the future

[13] ENISA, 'Guidelines for SMEs on the security of personal data', [Online']. Available: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing; ENISA, 'Security Measures', [Online]. Available: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/security-measures

use of sensors, wearables and drones, as well as the future citizen science platform, app and data collection. VUB-LSTS has also put legal and ethical considerations on paper per workshop which can be found on Nextcloud (SocioBee > WPs > WP2 > Workshops-Narrative).

For example, at the first workshop on sensors, wearables and drones, we pointed out that one must be extra careful with the sensors if one wants to record sound and image. For wearables that record location, explicit consent has to be given and for drones it is extremely important to look at exactly where you will be flying as there are various legal implications. Finally, we reminded them that citizen scientists need to be clearly informed before participating in the project.

At the second workshop on the SOCIO-BEE platform and the app, we listed legal and ethical considerations for 11 issues respectively. These include:

1. Legal and ethical considerations with respect to the SOCIO-BEE app(s)
2. Legal and ethical considerations with respect to the frequency of data collection by citizen scientists
3. Legal and ethical considerations with respect to the support that will be offered to the citizen scientists
4. Legal and ethical considerations with respect to the usage of data from Copernicus/satellites
5. Legal and ethical considerations with respect to how long it takes for citizen scientists to learn how to collect data
6. Legal and ethical considerations with respect to data curation and access to the data by the citizen scientists
7. Legal and ethical considerations with respect to digital tools for co-creation
8. Legal and ethical considerations with respect to push notifications to encourage participation
9. Legal and ethical considerations with respect to valorization mechanisms
10. Legal and ethical considerations with respect to survey participants about different information
11. Legal and ethical considerations with respect to storage of data collected through the app

2.8 Responsibility and resources

VUB, in close cooperation with the Project Coordinator (CERTH), the Project Manager (CERTH) and the External Ethics Advisory Board, will coordinate the efforts to characterize the nature and the type of the data produced, providing support to other partners in the consortium and ensuring standardization of the data and availability in the most appropriate scientific repository. This will be done in line with the standardization activities in WP8. Each SOCIO-BEE partner must respect the policies set out in this plan. Datasets must be created, managed and stored appropriately and in line with applicable legislation.

Furthermore, the SOCIO BEE partners involved in personal data processing will regularly keep records of the personal data processing activities carried out in the context of the project (Article 30 GDPR), including the kind of data, the department in charge, the specific purpose for which the data have been processed as well as the data storage periods.

2.9 Software tools

2.9.1 Consortium-wide tools

For collaborative work and as repository, the consortium uses NextCloud, as seen earlier. For communication, both a mailing list and a Slack workspace have been step up. For the regular plenary

telcos, the consortium uses GoToMeeting. Other partners also use MS Teams for the internal communication and co-creation tools, such as the Miro-Board.

2.9.1.1 CERTH

CERTH will be using the following software tools in SOCIO-BEE:

Tools for development purposes	Tools for DB management	Tools for reporting
• Python platforms (keras, Tensorflow etc.) • GIS • OpenAPIs/APIs • Javascript • C/C++ based IDE for hardware development • Python 3+ • Node JS 13 • HTTPS (HTTP over TLS) for secure connections • Angular2+	• MySQL • PostgreSQL • MongoDB	• Office automation suites (e.g. MS Office, etc.)

2.9.1.2 HYP

HYP will be using the following software tools in SOCIO-BEE:

Tools for development purposes	Tools for communication and collaboration	Tools for reporting
• Java • C# • C++ • Python • PHP • ASP.NET • HTLM5 • JavaScript	• Trustful third-party cloud services for email hosting	• Office automation suites (e.g. MS Office, etc.)

2.9.1.3 BETTAIR

BETTAIR will be using the following software tools in SOCIO-BEE:

Tools for development purposes	Tools for communication and collaboration	Tools for reporting
• Python platforms (keras, Tensorflow etc.) • GIS • OpenAPIs/APIs • C/C++ based IDE for hardware development	• MySQL • PostgreSQL • MongoDB	• Office automation suites (e.g. MS Office, etc.)

• Python 3+ • Node JS 13 • Node Red • Android studio		

2.9.1.4 VUB-SMIT

Tools for data collection purposes	Tools for communication and collaboration	Tools for reporting
• Prolific	• See 2.9.1	• See 2.9.1

2.9.1.5 UDEUSTO

Tools for development purposes	Tools for communication and collaboration	Tools for reporting
• -	• See 2.9.1	• See 2.9.1

2.10 Data protection legal requirements

The table below gives a brief overview of the status of the documents required for this deliverable. Given the number of documents collected and the information included in them, the documents are not included in the deliverable. However, all documents obtained from partners can be found in the project's repository, accessible in NextCloud.

The colours in the table mean the following:

- Presence is indicated by the colour blue
- If there is no input from the partner, this is marked in colour red
- If the process is not yet completed but has already started, this is marked in colour yellow
- If not applicable, it is indicated in colour grey

Furthermore, the different abbreviations for this table are listed below.

- **REP**: Research Ethics Protocol for SOCIO-BEE Researchers
- **DPO**: Data Protection Officer
- **DSP**: Data Security Protocol (or otherwise if applicable; **DPP**: Data Protection Policy)
- **TfIS & CF**: Templates for Information Sheets & Consent Forms
- **ECA**: Ethics Committees Approvals
- **D&W**: Drones & Wearables authorizations

Table 4. Overview of required documents for D1.5 from the partners in SOCIO-BEE

Partner	REP	DPO	DSP	TfIS & CF	ECA	D&W
ANCONA			DPP instead			
AUTH			DPP instead			
BETTAIR			DPP instead			
CERTH			DPP instead			
UDEUSTO			Both			
ECSA						

HKU						
HOPU	ISO 27001; ISO 9001		ISO 27001			
HYP			DPP instead			
IBER						
ID2M			DPP instead • French			
MRSI			DPP instead			
NILU						
UNIPD						
UNIVPM						
VUB						
ZGZ			DPP instead			
ZKF			DPP instead			

2.10.1 Data Protection Officers

The consortium will ensure that the partners processing personal data of research participants have, where applicable under the GDPR, appointed within their organizations a Data Protection Officer (DPO). The contact details will be made available to all data subjects involved in the research. Beneficiaries not required to appoint a DPO, based on GDPR provisions, must develop a detailed data protection policy for the SOCIO BEE project. Art. 24 of the GDPR states that "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary". "In other words, data protection policy is a set of principles, rules, and guidelines that informs how the organization will ensure ongoing compliance with data protection laws. The policies should recognize the data protection principles and the rights of individuals set out by the GDPR, and explain how they are put in to practice in relation to the processing carried out by the organization". [14]

Below is the list of the DPOs from the partners in SOCIO-BEE. If there is no input from the partner, this is marked in colour red.

Table 5. Data protection officers from the partners in SOCIO-BEE

Partner	Name of the DPO	Contact of the DPO
ANCONA	Dr. De Luca Davide	Email: privacy@pec.comuneancona.it Tel: 095 2935565
AUTH	Mrs. Cornelia Vikelidou	Email: data.protection@auth.gr Tel: 2310996200
BETTAIR	*N.A.*	Email: dpo@bettaircities.com
CERTH	Ms. Stella Papastergiou	Email: spapastergiou@certh.gr

[14] See: FASTER: D12.1 - POPD - Requirement No. 2 [DPOs and privacy policies for partners processing personal data], 2020., CO.

		Tel: +30 2310 498237
UDEUSTO	Mikel García Llorente	Email: dpo@UDEUSTO.es
ECSA	*N.A.*	*N.A.*
HKU	*N.A.*	Email: fg@hku.nl
HOPU	*N.A.*	Email: iris@hopu.org
HYP	Matina Tsiakoumi	Email: desk@hypertech.gr Tel: (0030) 210 6179441
IBER	Francisco Sanz	Email: ethics@ibercivis.es Tel: +34 976762995
ID2M	*N.A.*	Email: staff.gdpr@capinnove.be
MRSI	Mrs. Nikoletta Vlassiotou	Email: dpo@Amaroussion.gr Tel: 6944-327211
NILU		
UNIPD	Dr. Giorgio Valandro	Email: privacy@unipd.it
UNIVPM	Dr. Rosalba Sacchettoni	Email: rpd@univpm.it
VUB	*N.A.*	Email: dpo@vub.be
ZGZ	*N.A.*	Email: dpd@zaragoza.es
ZKF	Raquel Povar Saz	Email: rpovar@fundacionzcc.org

2.10.2 Data Protection Policy

As seen on the table above, almost all partners have provided their Data Protection Policies in line with the GDPR requirements. Those policies include information as to how personal data are handled inside each respective organisation. For SOCIO-BEE a customizable template has also been prepared which will serve as a guideline for partners who currently do not have a data protection policy, because this is not required by law. **This template can be found in Annex III – Data Protection Policy.**

2.10.3 Data Protection Notice

A draft template for the Data Protection Notice Template for the website or other activities is also provided. "A privacy notice is a public document from an organization that explains how that organization processes personal data and how it applies data protection principles. Articles 12, 13, and 14 of the GDPR provide detailed instructions on how to create a privacy notice, placing an emphasis on making them easy to understand and accessible". The template can be found in **Annex II – Data Protection Notice Template for the website or other activities**.

2.10.4 Data Security Protocol

As part of the DMP, a Data Security protocol is also expected to be developed. For this initial version of the DMP, as seen on the table above, almost all partners have provided a Data Security Protocol, either as a stand-alone policy/standard certification or as part of their Data Protection Policies. The Protocols provide information on data security themes that partners need to follow within the SOCIO-BEE project to help protect (sensitive) data since both technical and operational security must be strong. For SOCIO-BEE, VUB also provided a Data Security Protocol template with fundamental data security principles,

which **can be found in Annex IV – Data Security Protocol.** More details about this Protocol and the need to further specify it will be re-visited in the next version of the DMP, also in line with WP3.

2.10.5 Data Protection Impact Assessment

A Data Protection Impact Assessment is envisaged in Article 35 of GDPR and will take place in WP6 in SOCIO-BEE as part of the holistic impact assessment. Its rationale, methodology and methods to be used will be defined in D6.1 and the reporting of the analysis will take place in D6.2 and D6.3.

2.10.6 Joint Controllership Agreement

In the SOCIO BEE context, there may be cases where consortium partners undertake the role of independent data controller or data processor. However, in other cases, consortium partners involved in personal data processing may be joint controllers, whenever they will jointly determine the purposes and means of the personal data processing operations. For that purpose, In the previous D1.5, a general first draft version of a Joint Controllership Agreement was included. **This template can be found in Annex V – Joint Controllership Agreement.**

In preparation for the pilots, the involved partners executed a joint controllership arrangement, which is included as Annex VI.

This initial assessment will be further validated or modified, as necessary, by using amendments. In that case, any changes will be documented in future deliverables.

2.10.7 Data processing by external entities

Moreover, the partners may hire external entities or may deploy the services of external entities for data processing purposes (for instance, for storage purposes) along the course of the project. No processing will take place until the necessary data processing agreements are in place. Often, such agreements will be automated (the partners will not be able to use the tool without accepting the terms and conditions). In other cases, the partners may indeed have to enter into a negotiation phase with the vendor/operator.

2.10.8 Intellectual property

It is also expected that partners will generate Intellectual Property that has to be protected through patents, made available for other partners for their own work in the project, and exploited outside of the project by appropriate routes. The management of the project knowledge and of the IPRs is specified in the Consortium Agreement that has been signed by the Partners. Its content reflects and in some cases complements the terms and conditions defined in the Commission Contractual Rules. More specifically the Consortium Agreement covers topics such as Individual and Joint Ownership of the knowledge, Protection of knowledge, Publication of results, Use and dissemination of knowledge arising from the project, access rights, Open Source and Standards, etc. The provision of an effective "intellectual property protection for knowledge capable of industrial or commercial application" is considered a clear obligation of the Partners of the Consortium. The Consortium Agreement specifies in detail the rules and obligations regarding existing expertise and knowledge developed during the project.[15] More work on that, is planned to take place as part of the exploitation and standardization component of the project (WP1 and WP8).

[15] See: SOCIO-BEE: D1.4 – Project Handbook, p. 35

2.11 Pilots

In preparation for the pilots, as detailed under WP5, the partners have adopted a number of measures to ensure the adequate implementation of the DMP. In this respect, the partners have adopted:

- a joint controllership arrangement;
- an informed consent form;
- an information sheet;
- a research ethics protocol;
- a privacy notice;
- an end user license agreement.

2.11.1 Joint Controllership Agreement

In preparation for the pilots, the involved partners executed a joint controllership arrangement, which is included as Annex VI.

2.11.2 Informed consent form

Considering the different intended audiences for the pilots, it was decided to settle on consent as legitimate basis for the processing of the personal data involved in the pilot. The final document used can be found in Annex VIII.

2.11.3 Information sheet

In line with the previous document, an information sheet was drafted to secure an informed consent from the pilots' participants. The final document can be found in Annex VIII.

2.11.4 Research ethics protocol

Given the novelty of the citizens' science approach, it was decided to produce a document that explains to participants their role as citizen scientists. The final document can be found in Annex VII.

2.11.5 Privacy notice for app

Since the ACADE-ME app will process personal data, it was decided to draft a privacy notice, following the template in Annex II. The final document can be found in Annex X.

2.11.6 End user license agreement

Finally, considering that the citizen scientists would have to use the ACADE-ME app for their participation, and also taking into consideration the legal requirements put in place by the distribution app store involved, it was drafted an end user license agreement to provide a non-exclusive and free license for the lawful use of the app during the pilots. The final document can be found in Annex XI.

3 Ethical Management Plan

3.1 Introduction

The Ethical Management Plan will provide an overview of the good practice guidelines for SOCIO-BEE Consortium members concerning ethical standards. It additionally details key steps and procedures in

relation to carrying out the SOCIO-BEE project to a high standard and in accordance with European and international guidelines for ethical conduct in research practice. The Ethical Management Plan will partly be based on various works such as the PRO-RES Framework and PRINTEGER Project and also on D6.1 Ethical Management Plan of SEEDS (Science Engagement to Empower Disadvantaged Adolescents). Those projects have made extensive work on research ethics and give a good overview of the European requirements and where necessary, reference will be made to them in the footnotes.

3.1.1 Obligation to comply with ethical and research integrity principles (G.A. Art. 34.1)

As defined in the G.A. H2020, all SOCIO-BEE activities and the partners must implement the action in accordance with[16]:

- ethical principles (including the highest standards of research integrity) and
- applicable international, EU and national law.

"In addition, the beneficiaries must respect the fundamental principle of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity".[17] This implies compliance with the following fundamental principles:

- **reliability** in ensuring the quality of research reflected in the design, the methodology, the analysis and the use of resources;
- **honesty** in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair and unbiased way;
- **respect** for colleagues, research participants, society, ecosystems, cultural heritage and the environment;
- **accountability** for the research from idea to publication, for its management and organization, for training, supervision, and mentoring, and for its wider impacts

and means that beneficiaries must ensure that persons carrying out research tasks follow the good research practices and refrain from the research integrity violations described in this Code. This does not change the other obligations under the GA or obligations under applicable international, EU or national law, all of which still apply". The European Code of Conduct for Research Integrity "describes professional, legal and ethical responsibilities, and acknowledges the importance of the institutional settings in which research is organised. Therefore, this Code of Conduct is relevant and applicable to publicly funded and private research, whilst acknowledging legitimate constraints in its implementation".[18]

3.1.2 Activities raising ethical issues (G.A. Art. 35.1)

If certain activities in SOCIO-BEE cause potential ethical issues, they will have to comply with the 'ethical requirements' first cited in this Ethical Management Plan and in further deliverables in Work Package (WP) 6.

> "Before the beginning of an activity raising an ethical issue, each beneficiary must have obtained:
> - any ethics committee opinion required under national law and

[16] G.A., p. 53 - 54
[17] ALLEA ALL European Academies (2017). *'The European Code of Conduct for Research Integrity Revised Edition'*. Berlin: All European Academies; 2017, [Online]. Available: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf
[18] Ibid., p. 3

- any notification or authorization for activities raising ethical issues required under national and/or European law

needed for implementing the action tasks in question.

The documents must be kept on file and be submitted upon request by the coordinator to the Agency.[19] If they are not in English, they must be submitted together with an English summary, which shows that the action tasks in question are covered and includes the conclusions of the committee or authority concerned (if available)". [20]

3.1.3 Applicable ethical and legal requirements in SOCIO-BEE

Ethics is given the highest priority in the European Union (EU) funded research and thereby all SOCIO-BEE activities must be conducted according to applicable international, EU and national legal and ethical requirements. For SOCIO-BEE, this means on a national level for the participating countries: Belgium, Germany, Greece, Italy and Spain. These will be shown further in 'Table 6. - Relevant national laws and regulations in partners' countries', where we emphasize on personal data protection law and ethics guidelines. The following guidelines below intent to aid all SOCIO-BEE members during the project and promote a shared understanding of the importance of high standards in research and adherence to guidelines concerning ethical conduct in research:[21]

SOCIO-BEE will have to comply with the following ethical principles:

- The European Commission's Online Manual on Ethics (2022)[22]
- The European Commission's Ethics on Social Sciences and Humanities (2018)[23]
- The European Commission's Ethics and data protection (2018)[24]
- The European Commission's comprehensive guidelines Ethics for Researchers: Facilitating Research Excellence in Seventh Framework Programme FP7 (2013)[25]
- The European Code of Conduct for Research Integrity: Revised Version (2017)[26]; and
- Best Practices for Ensuring Scientific Integrity and Preventing Misconduct, a set of guidelines issued by The Organization for Economic Co-operation and Development (OECD)'s Global Science Forum (2007)[27]

[19] See: G.A. Art. 52
[20] See: G.A., p. 54
[21] See: SEEDS: D6.1 – Ethical Management Plan, 2021, [Online]. Available: https://seedsmakeathons.com/wp-content/uploads/2021/12/SEEDS-Ethical-Management-Plan-March-2021.pdf, p . 7
[22] See: https://webgate.ec.europa.eu/funding-tenders-opportunities/display/OM/Online+Manual
[23] European Commission, 'Ethics in Social Science and Humanities', 2018 [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf
[24] European Commission, 'Ethics and Data Protection', 2018, [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
[25] European Commission, 'Ethics for Researchers: Facilitating Research Excellence in Seventh Framework Programme FP7, [Online]. Available: https://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf
[26] Ibid.
[27] OECD, 'Best Practices for Ensuring Scientific Integrity and Preventing Misconduct', 2007, [Online]. Available: http://www.oecd.org/science/inno/40188303.pdf

- Rules for Participation: Ethics (Article 19)[28]

SOCIO-BEE will have to comply with the following fundamental rights instruments:

- Charter of Fundamental Rights of the EU (2012/C 326/02)[29]
- The European Convention on Human Rights[30]

SOCIO-BEE will have to comply with all applicable legal requirements, including but not limited to:

- The General Data Protection Regulation
- The e-Privacy Directive and the subsequent e-Privacy regulation
- Legislation about drones, wearables and sensors (See D3.1)

Moreover, SOCIO-BEE follows the national regulations shown in Table 6.

Table 6. Relevant national laws and regulations in partners' countries

Partners of SOCIO-BEE Consortium	Relevant National Laws and Regulations
Belgium • ID2MOVE • VUB	**GDPR** • The Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data • Act of 3 December 2017 establishing the Data Protection Authority **Ethics** • The European directive 2001/20 has been incorporated in national law by the law dated 7th May 2004 published in the Belgian Monitor of 18th May 2004. The new legal framework has been in force since 1st May 2004. ○ The law of 7 May 2004 has been modified several times
Germany • ECSA	**GDPR** • Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June 2017 • "In addition to the BDSG, there exist a number of data protection rules in area-specific laws, for example those regulating financial trade or the energy sector. Many of these laws have been adapted to the GDPR by the Second Data Protection Adaptation and Implementation Act EU (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – '2. DSAnpUG-EU'), which generally entered into force on November 26, 2019. " **Ethics** • The National Council for Ethics: http://www.ethikrat.org/ ("Deutscher Ethikrat") (not binding)
Greece • AUTH • CERTH • HYP	**GDPR** • Law 4624/2019 which also contains provisions for the implementation of Directive (EU) 2016/680 and other provisions (Data Protection Act 2019**)** **Ethics**

[28] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/201, *OJ L 170, 12.5.2021, p. 1–68*

[29] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, [Online]. Available: https://www.refworld.org/docid/3ae6b3b70.html

[30] European Court of Human Rights, 'European Convention on Human rights', [Online]. Available: https://www.echr.coe.int/documents/convention_eng.pdf

• MRSI	- The most recent Act 3653/2008 on Research and Technology, albeit it refers to the evaluation of research protocols, does not make any reference to the role of Ethics Committees in this evaluation.
Italy • ANCONA • UNIPD • UNIVPM	**GDPR** • Italian Personal Data Protection Code (Legislative Decree 196/2003), Amended by Legislative Decree 101/2018 • Legislative Decree n. 101/2018 **Ethics** • The Ministerial Decree 8 February 2013 stating the reorganization of Ethics Committees in Italy, member characteristics and background: so called Decreto Balduzzi
Norway • NILU	**GDPR** • The GDPR was incorporated in the EEA Agreement by a Joint Committee Decision dated July 6, 2018. The new Norwegian Personal Data Act (LOV-2018-06-15-38) ("PDA") implements GDPR and became effective as of July 20, 2018. **Ethics** • Research Ethics Act (2017)[31]
Spain • UDEUSTO • BETTAIR • ZKF • IBER • ZGZ • HOPU	**GDPR** • Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (“Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”) (the “Data Protection Act”) **Ethics** • National Statement on Research Integrity, 2 December 2015 by the CSIC, the Conference ofRectors of Spanish Universities (CRUE) and the Confederation of Spanish Scientific Societies. • Law 14/2011, of June 1, on Science, Technology, and Innovation, BOE n.131, adopted 2-06-2011. • The Spanish Research Ethics Committee (Comité Español de Ética de la Investigación, CEEI). Created by the Law of Science, under the Council for Science, Technology and Innovation Policy. • Spanish National Research Council (Consejo Superior de Investigaciones Científicas, CSIC),CSIC Code of Good Scientific Practices, 2011 CSIC. • The Spanish Science and Technology Foundation (Fundación Española para la Ciencia y Tecnología, FECYT).
The Netherlands • HKU	**GDPR** • The Implementation Act (Uitvoeringswet AVG) **Ethics** • Code of Good Conduct (in Dutch: Code Goed Gedrag)

[31] See: https://lovdata.no/dokument/NL/lov/2017-04-28-23?q=forskningsetikk

3.2 Good research practice guidelines

The SOCIO-BEE Consortium joins together a group of experienced researchers from different European countries, and all of them agree to adhere to the principles of integrity of research and good practice in research throughout the entire project. The European Code of Conduct for Research Integrity: Revised Version, issued in 2017, provides good research practices based on the four aforementioned principles of integrity in research.

3.2.1 Good research practice in different research contexts applied to SOCIO-BEE project

3.2.1.1 The European Code of Conduct for Research Integrity: Revised Version

All the researchers from the different European countries agree to adhere to the principles of integrity of research and good practice throughout the entire project as stated in the G.A. They will therefore comply to the previously mentioned 'The European Code of Conduct for Research Integrity: Revised Version', issued in 2017, which provides good research practices based on the four principles of integrity in research. [32] The Good Research Practices are defined by different research contexts into specific activities that will be developed in SOCIO-BEE[33]:

I. **Research environment**:
   - Research institutions, organizations and companies participating in the Consortium of SOCIO-BEE will ensure the prevailing culture of research integrity, the provision of clear policies and procedures on good research practice, the support of proper infrastructure for the data management and data protection, and the reward hiring and promotion of researchers when they applied open and reproducible practice.

II. **Training supervision and mentoring**:
   - Research institutions, organizations and companies participating in the Consortium of SOCIO-BEE will ensure that researchers received rigorous training in research (design, methodology and analysis of data) and in ethics integrity.

III. **Research procedures**:
   - Researchers from SOCIO-BEE will consider the state- of-the art in developing research ideas, design and analyze the project and specific activities carefully and in a well-considered manner, use the research funds properly, respect the data confidentiality and publish results in an open-access and transparent manner, and they report the results in a reproducible way.

IV. **Safeguards**:
   - Researchers from SOCIO-BEE will comply with the discipline' codes and regulations, address human subjects with respect and care based on ethical SOCIO-BEE guidelines, considering health, safety and welfare of the community and project' participants (children, adolescents, elderly, and stakeholders), be sensitive considering the differences

[32] ALLEA ALL European Academies (2017). 'The European Code of Conduct for Research Integrity Revised Edition'. Berlin: All European Academies; 2017, [Online]. Available: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf

[33] SEEDS: D6.1 – Ethical Management Plan, 2021, [Online]. Available: https://seedsmakeathons.com/wp-content/uploads/2021/12/SEEDS-Ethical-Management-Plan-March-2021.pdf, p. 10 - 11

among participants (ethnic, religion, age, culture, gender and socioeconomic level), and manage the risks and harms of the SOCIO-BEE research.

V. **Data practices and management**:
   - Research institutions, organizations and companies participating in the Consortium of SOCIO-BEE will ensure appropriate data protection, open-access data when it is possible, as closed as necessary, and where appropriate in line with the FAIR Principles (Findable, Accessible, Interoperable and Re-usable) for data management, be transparent on how to access or use this data, acknowledge data is legitimate and citable products of the research, ensure the protection of intellectual property in any contracts and agreements relating to research outputs. This information is mentioned in the above section 2 of the Data Management Plan.

VI. **Collaborative working**:
   - Researchers of SOCIO-BEE in their research collaborations will take responsibility for the integrity of the research, agree at the beginning the goals of the research, the process to communicate it, the laws and regulations that apply them, and properly informed of the submission of results publications.

VII. **Publication and dissemination**:
   - All authors of SOCIO-BEE will be fully responsible for the content of the publications derived from the project, agree on the authorship publications guidelines specified in the Grant Agreement and Project Management Handbook of SOCIO-BEE, acknowledge their work to others (collaborators, assistants and funders), disclose any conflicts of interest and financial or other types of support for the research or for the results' publication, commit to correct or retract work if necessary, consider negative findings as valid as positive results for publication and dissemination and, made available their work related to the project timely, open, transparent and in an accurate manner.

VIII. **Reviewing, evaluating, and editing**:
   - Researchers of SOCIO-BEE will commit to participate in refereeing, reviewing, and evaluating submissions for publications, funding, appointment, promotion, or reward in a transparent and justifiable manner. Moreover, reviewers or editors with a conflict of interest will withdraw from the publication decision, funding, appointment, promotion or reward and they will maintain the confidentiality unless approval for disclosure was prior.

3.2.1.2 Other relevant Research Ethics and Research Integrity Projects

Previous work programs within the Science for and with Society (SwafS) provided projects that produced Research Ethics (RE) and Research Integrity (RI) guidelines and regulatory frameworks, among others. Below are projects that serve as a reference for the SOCIO-BEE Ethical Management Plan:

PANELFIT – 'Participatory Approaches to a New Ethical and Legal Framework for ICT'

PANELFIT (G.A. No 788039, 1 Nov 2018 – 30 April 2022) "is a H2020 EU funded project aiming at facilitating the adaptation processes between new technical advances and legal frameworks, by producing a set of editable, openly accessible guidelines, as well as offering operational standards capable of reducing

ethical and legal problems posed by information and communication technologies"[34]. Some of the outcomes (deliverables) of PANELFIT can be useful for SOCIO-BEE, namely:

- Guidelines on the ELI of ICT research and innovation;
- Code of Conduct for RRI[35]
- Issues and gaps analysis on informed consent in the context in ICT research and Innovation[36]

PRINTEGER – 'Promoting Integrity as an Integral Dimension of Excellence in Research'

PRINTEGER (G.A. No 665926, 1 Sep 2015 – 31 Aug 2018) is a H2020 EU funded project. "Its mission is to enhance research integrity by promoting a research culture in which integrity is part and parcel of what it means to do excellent research, and not just an external and restrictive control system. To promote such a culture, an improved governance of integrity and responsible research has to be informed by practice: the daily operation of researchers and the tensions of a complex research system. PRINTEGER will contribute to improve adherence to high standards of integrity in research warranting high levels of public support for the sciences. In the short term, it will do so by improving integrity policies of national and international research organisations, but also by providing better tools for research leaders and managers. In the longer term, PRINTEGER will contribute to improve ethical awareness and reflection through the education of new generations of scientists with next generation educational tools".[37] Some of the outcomes (deliverables) of PANELFIT can be useful for SOCIO-BEE, namely:

- Bonn PRINTEGER statement: Working with Research Integrity—Guidance for research performing organisations [38] [39]

"The aim of the statement is to complement existing instruments by focusing specifically on institutional responsibilities for strengthening integrity. [40] It takes into account the daily challenges and organisational contexts of most researchers. The statement intends to make research integrity challenges recognisable from the work-floor perspective, providing concrete advice on organisational measures to strengthen integrity. The statement provides guidance on the following key issues":

- § 1. Providing information about research integrity
- § 2. Providing education, training and mentoring
- § 3. Strengthening a research integrity culture
- § 4. Facilitating open dialogue
- § 5. Wise incentive management
- § 6. Implementing quality assurance procedures
- § 7. Improving the work environment and work satisfaction
- § 8. Increasing transparency of misconduct cases

[34] PANELFIT, 'Objectives', [Online]. Available: https://www.panelfit.eu/objectives-outcomes/
[35] PANELFIT: D5.4 - Code of Conduct on Data Protection for Responsible Research and Innovation v3.0, 2021, [Online]. Available: https://www.panelfit.eu/wp-content/uploads/2021/03/Panelfit-Code-of-Conduct-on-Data-Protection-CCDP.pdf
[36] PANELFIT, 'D2.1 - Issues and gaps analysis on informed consent in the context in ICT research and Innovation', 2020, [Online]. Available: https://www.panelfit.eu/wp-content/uploads/2020/11/D21-Issues-and-gaps-analysis-on-informed-consent-in-the-context-in-ICT-research-and-Innovation.pdf
[37] PRINTEGER, 'About', [Online]. Available: https://printeger.eu/
[38] PRINTEGER, 'The Bonn PRINTEGER Statement, [Online]. Available: https://printeger.eu/the-bonn-printeger-statement/
[39] Forsberg, E.-M., et. al. (2018). Working with Research Integrity—Guidance for Research Performing Organisations: The Bonn PRINTEGER Statement. *Science and Engineering Ethics*, *24*, p. 1023-1034. doi:10.1007/s11948-018-0034-4
[40] Complementing existing instruments such as the European Code of Conduct for Research Integrity

- § 9. Opening research
- § 10. Implementing safe and effective whistle-blowing channels
- § 11. Protecting the alleged perpetrators
- § 12. Establishing a research integrity committee and appointing an ombudsperson
- § 13. Making explicit the applicable standards for research integrity

PRO-RES - 'Promoting integrity in the use of research result'

PRO-RES (GA No 788352, 1 May 2018 – 31 Oct 2021) "is a European Commission-funded project aiming to PROmote ethics and integrity in non-medical RESearch by building a supported guidance framework for all non-medical sciences and humanities disciplines adopting social science methodologies".[41] This normative framework for ethical evidence consists of three parts, namely: 1) a statement (The Accord) for all who are concerned to ensure policies are based upon ethical evidence 2) a toolbox to supplement and operationalize the Accord to identify ethical evidence that supports decision-making 3) additional supportive resources that complement the Accord and the Toolbox. For SOCIO-BEE, the toolbox will be particularly useful in order to make a judgment about how ethically the research/analysis was conducted and if the researchers/analysts/advisors behaved with integrity.

3.3 Citizen science ethics

Citizen science is further explored and supported under the SWAFS Work Programme 2018-2020 (WP18-20), 'Strategic orientation 4. Exploring and supporting citizen science'. This Work Programme was "developed to reflect and support the evolution of science and society and the increased emphasis on their interplay at national and EU levels. There is recognition that co-design with citizens, stakeholders and end-users needs to be promoted in all policy instruments, including in Horizon 2020".[42] Citizen science is also part of open science which constitutes a "new approach to the scientific process based on cooperative work and new ways of diffusing knowledge by using digital technologies and new collaborative tools".[43] This includes citizen science as the sharing and (re)use of data and knowledge throughout the scientific process is central.[44] "The strong connection between Open Science and research integrity has been underlined in the Council conclusions on research integrity, where the Member States recognize the importance of open science as a mechanism for reinforcing research integrity, while, at the same time, research integrity contributes to open science.[45] [46]

The active participation of citizens in science and innovation is growing rapidly and can provide many benefits where traditional research falls short, but some considerations must also be kept in mind such as:

[41] PRO-RES, [Online]. Available: https://prores-project.eu/
[42] European Commission Decision C(2020)6320 of 17 September 2020), Work Programme 2018-2020, 16. Science with and for Society, [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-swfs_en.pdf, p. 16
[43] Ibid., p. 16
[44] European Commission, 'Open innovation, open science, open to the world - a vision for Europe', [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/open-innovation-open-science-open-world-vision-europe
[45] Ibid.
[46] Ibid.

- Ethical and regulatory considerations including: concerns regarding the protection of participating citizens, their potential exploitation, the collection of big data and related privacy considerations, as well as intellectual property issues"[47];
- "Involvement of citizen scientists must be in line with Article 21 of the Charter of Fundamental Rights of the European Union, e.g. regardless of sex, age, social origin. To improve science-society relations, efforts should be made to include all parts of society, including hard-to-reach and vulnerable groups, in citizen science activities"[48]

When considering the extent to which citizen science can be considered ethical, there is an important issue to consider. Citizen science, because of its alternative, new forms of conducting research and generating knowledge, produces new roles, boundaries and relationships between the researchers and citizen scientists. Research shows that because of these characteristics, citizen science is currently not sufficiently covered by ethical and regulatory requirements.[49] This is particularly evident in the case of existing regulatory mechanisms. As Tauginienė et al. (2021) stated: "while the protection of human subjects in research has traditionally been guided by informed consent or Institutional Review Board (IRB) mechanisms, the widely distributed nature of citizen science challenges a one-size-fits-all set of ethical requirements for the broad variety of practices and collaborative formats that it embraces (…). Also, many citizen science projects count on the collaboration of research participants who are not the primary subjects of research (…) since research participants become both subjects and objects of research and may interact with researchers as equals in the research process". [50] This issue is then expressed in three different ways, namely:

- There is a focus on the protection of the rights and welfare of 'passive' research subjects;
- It is built on the paternalistic assumption that research participants may not be able to correctly assess the harms and benefits involved in the research process;
- The vast amounts of data collected, aggregated, and repurposed in citizen science projects imply a degree of uncertainty about the outcomes, which could evolve over time.

So new forms of informed consent are needed. For this, Tauginienė et al. (2021) propose to introduce the model of *dynamic informed consent.* It's "a strategy to involve participants, support the principle of informed consent, and solve the 'stationary' aspect of consent, via a technological construct such as a communication platform that establishes a continuous two-way communication between researchers and participants".[51]

Furthermore, the authors note that citizen science has both conceptual and practical ethical challenges. Some of these challenges include (non-exhaustively)[52]:

[47] Ibid., p. 42
[48] Ibid., p. 45
[49] Rasmussen, L. M., & Cooper, C. (2019a). Citizen science ethics. *Citizen Science: Theory and Practice, 4*(1), 5. https://doi.org/10.5334/cstp.235; Fiske, A., del Savio, L., Prainsack, B., & Buyx, A. (2018). Conceptual and ethical considerations for citizen science in biomedicine. In N. B. Heyen, S. Dickel, & A. Brüninghaus (Eds.), *Personal health science* (pp. 195–217). Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-16428-7_10617. https://doi.org/10.1136/medethics-2018-105253
[50] Resnik, D. B. (2019). Citizen scientists as human subjects: Ethical issues. *Citizen Science: Theory and Practice, 4*(1), 11. https://doi.org/10.5334/cstp.150
[51] Tauginienė, L., et al. (2021). Ethical Challenges and Dynamic Informed Consent. In: K. Vohland et al. (eds.), *The Science of Citizen Science* (pp. 397–416). Springer, Cham. P. 398-399
[52] Ibid.

- Instrumentalization
- Exploitation
- Inclusiveness
- Research Malpractice
- Collaboration with Private Partners
- Payment and Free Labour
- Ownership and Acknowledgement

Dynamic informed consent could be a potential solution to some of these ethical challenges. It is important to keep an eye on these issues throughout the SOCIO-BEE project because "fostering a high ethical standard for citizen science is crucial to its success as its practice will allow for better experiences for participants and potentially more sustainable projects".[53] The pilots' results will inform a decision for the final deliverables and outputs of the project.

3.3.1 Open data and citizen science

From the European level, open data is promoted both to give society at large access to data and for research integrity. "However, it remains unclear whether open data should be reused without informed consent. It goes without saying that there is a clear tension between the ideals of openness and accessibility that citizen science promotes and participants' interests related to data protection".[54]

Citizen Science poses several implications with respect to the data protection legal framework, mainly due to its openness and its decentralized character.[55] Researchers working for official research institutions or academia, in order to conduct trials and experiments, have to abide by very strict standards, for instance go through lengthy ethics procedures to have their research designs and protocols approved. Respectively, during the actual research implementation stage, research takes place usually by highly specialized experts, who have to follow precise methodologies and specific codes of conducts and principles of research integrity, retain a level of transparency, disclose information about possible conflicts of interest or funding, appropriately publish their results and ensure the datasets can be re-used to ensure repeatability and verifiability – all these in line with strict laid out legal and ethical requirements. Comparatively, in the context of citizen science, despite the existence of some underlying principles, there is a degree of informality and flexibility, leading to questions such as: who oversees a trial and who is the data controller? Can in some cases citizen science be simply a household activity which would be exempt from the GDPR application? And who can data subjects whose rights have been violated turn to?

Overall, the GDPR does provide special and sometimes seen as more privileged conditions for the processing of personal data when the latter are used in the context of scientific research, as compared to other purposes, due to a general perception that this is important for the common good.[56] Scientific research is not defined in GDPR. The European Data Protection Board has adopted Guidelines in this

[53] Ibid., p. 399
[54] Ibid, p. 410
[55] A Berti Suman and R Pierce, 'Challenges for Citizen Science and the EU Open Science Agenda under the GDPR' (2018) 4 European Data Protection Law Review 284.
[56] Paul Quinn, 'Research under the GDPR - a Level Playing Field for Public and Private Sector Research?' (2021) 17 Life Sciences, Society and Policy 4.

regard to shed light on the interplay between scientific research and data protection law, with respect to health.[57] [58]

3.4 SOCIO-BEE ethical guidelines

Within the SOCIO-BEE project, the ethical standards and guidelines of Horizon 2020 will be rigorously applied, regardless of the country in which the research is carried out.[59]

3.4.1 Ethics commitments in SOCIO-BEE

Based on the ethics self-assessment in the SOCIO-BEE proposal, the SOCIO-BEE consortium prepared an Ethics Commitments Strategy to be followed throughout the project lifecycle, starting already from the proposal. The Strategy can be found in table below. The table also shows the status of each commitment. Two types of classification are provided for this purpose, namely:

- *[Finished]*
- *[In progress]*

Table 7. Updated SOCIO-BEE's Ethics Commitments Strategy

SOCIO BEE's Ethics Commitments Strategy		
Strategies	**Deadline**	**Status**
Kick-off Law & Ethics Workshop	[M01]	*Finished:* *During the kick-off meeting, VUB in cooperation with the Project Coordinator organized an 1-hourr Law and Ethics Workshop, where VUB presented an outline of the main legal and ethical requirements with respect to the project research activities and accommodated questions and concerns, which were later ffed into D3.1.*
Establishment of the project's External Ethics Advisory Board (EEAB) withinternal and external partners	[M03]	*Finished:* *The EEAB is part of the EAB, which was formed in the beginning of the project.*
Confirmation of the EEAB's *modus operandi* and organization of annual and adhoc meetings Designation of a Gender, Ethics, Law and Privacy Manager (GELPM) with a Gender and Inclusion expert (UDEUSTO) and a Privacy, Legal and Ethics Expert	[M06] • Confirmation of the EEAB's *modus operandi* [Regularly] • Organization of annual and ad hoc meetings	*In progress:* • *Establishment of annual meetings coinciding with the annual plenary meetings*

[57] https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf
[58] SOCIO-BEE, 'D3.1 - Report on Legal and Regulatory Requirements_v1.8, p. 23 - 24
[59] European Commission, 'Horizon H2020 Online Manual. Ethics. European Commission', [Online]. Available: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cuttingissues/ethics_en.htm

(VUB). WP6 supports this purpose.		
Provision of all relevant permissions/authorizations and approvals from Ethics Committees	[M06] and possible updates throughout the project life cycle	*In progress:* – *first reporting in M06 in D1.5 after bilateral telcos with all the partners and documentation received by them*
Data Management Plan (DMP) and updates	[M06/ M20/ M36]	*Initial report submitted in M06*
Data Security protocol, including technical and organizational measures (part of the DMP)	[M06]	*In progress*
Provision of templates for Information Sheets and Consent Forms for participation in SOCIO BEE research [proposal]	[Proposal]	*Finished* • *Drafts in proposal – see Section 5, p. 73 - 74* *In progress:* • *support of partners to prepare customized information sheets and consent forms per case*
Development of the SOCIO BEE Ethics Research Protocol	[M06 or in any case before any research activities take place]	*In progress:* – *collection of partners' ethics protocols or other relevant and corresponding documentation* – *assessment as to whether a common protocol is necessary or not*
Development of the SOCIO BEE Ethics Research Protocol for citizen scientists Engagement of organizations' DPOs or whenever the appointment of a DPO is not compulsory, drafting of a specific data protection policy for the project (contact details of DPOs and data protection policies will be part of the DMP) [M06]	[M06 or in any case before any research activities take place]	*Finished:* • *Ethics Research Protocol for citizen scientists (first version finished, available in D1.5)* • *Collection of DPOs' contact information contacts)*
Records of all the personal data processing activities kept internally by the partners	[Regularly]	*In progress*
Conduct of an Impact Assessment • co-design of a tailor-made template • 2 reports: before and	[M12, M35] • 2 reports: To be coordinated: • 2nd Law and Ethics Workshop	*In progress: Methodology in preparation (D6.1)*

after the pilots • 2nd Law and Ethics Workshop after the first report		
Formation and fulfilment of 'legal and ethical' KPIs Launch of Knowledge Powerhouse on legal and ethical matters in relation to citizen science on the project website [M32]	[regularly] • Legal and ethical KPIs [M32] • Launch of Knowledge Powerhouse	*In progress*

3.4.2 Gender, Legal, Privacy and Ethics Managers

3.4.2.1 Legal, Privacy and Ethics (VUB-LSTS)

The Legal, Privacy and Ethics manager will be responsible for ensuring that all actions and activities within the project have a gender-sensitive approach and are conducted following established ethical principles, including the highest standards of research integrity, and applicable international, EU and national guidelines and legislation. This role has been assigned to VUB. VUB leads the WP on Law and Ethics.

3.4.2.2 Gender focal point

According to UN Women Training Centre, the role of a Gender Focal Point is to "advocate for increased attention to and integration of gender equality and women's empowerment in the agency's policy and programming" (UN Women Training Centre 2016). This task is also aligned with EU policy and the EU Strategy for Gender Equality. Therefore, the task of the Socio Bee Gender Focal Point will be to check that all participating institutions have/implement a GEP; to provide training and technical support when needed for the inclusion of gender issues in Socio Bee activities and outputs; and to assist the project coordinator on the drafting of the gender analysis for the periodic reports. Moreover, the GFP will make sure that participation in project activities is gender-balanced, and that data are disaggregated and relevant for all groups and will be the contact person in case of sexual harassment.

3.4.3 External Ethics Advisory Board (EEAB)

This is a sub-group of the External Advisory Board (EAB), which consist of three EAB members with proven expertise in legal and ethical matters, the Project Coordinator (PC) as General Assembly (GA) Chair, a designated member from the Steering Committee (SC) and the GPLEM. The EEAB will convene regularly once per year upon the occasion of the annual consortium plenary meeting and will be chaired by the GPLEM. Any decisions of the EEAB will be taken based on an absolute majority vote scheme. The EEAB Chair does not have the right to vote. During its regular operations, the EEAB will review the consortium efforts and provide opinions on legal and ethical matters or disagreements thereof, ensuring the most effective implementation of the legal and ethical requirements and the high quality of relevant deliverables and procedural aspects during the project lifecycle. The EEAB may convene outside its regular operation to address ad hoc matters of outmost importance, after request of an EAB member, the PC, the

designated SC member or the GPLEM. The EEAB Chair will keep the minutes and subsequently report about EEAB's activities to the EAB and the rest of the consortium, after each meeting. The minutes and other accompanying documents will be stored securely in the project repository, alongside their degree of confidentiality.[60]

The Board, amongst others, will ensure that the SOCIO- BEE activities are carried out, in line with:

- The protection of human research participants from any physical or mental discomfort, or from danger, intrusion, or harm that may result from particular research procedures;
- Safeguards for the project's reputation for the research that it conducts and sponsors;
- Efforts for minimizing the potential for breaches of legislation and for claims of negligence that might be brought against the researcher and the project

3.4.4 Development of the SOCIO BEE Research Ethics Protocol

Most partners have various forms of what can be broadly described as 'research ethics protocols'. Depending on the entity of the partner, this can differ between visions / statements / missions of companies or organizations or, for example, a 'research data management policy framework' and policy regarding 'open accesses at universities and research institutions. This collection took place together with the other legal and ethical requirements as indicated in Table 4 'Overview of required documents for D1.5 from the partners in SOCIO-BEE'. As the project progresses, it will become clear whether there is still a need for a common protocol or not. This will be added in the second DMP in M20 and made before the start of the pilots if necessary.

3.4.5 Citizen science principles

3.4.5.1 Research Ethics Protocol for Citizen Scientists

As laid down in the SOCIO-BEE's ethics commitments strategy, a Research Ethics Protocol for Citizen Scientist is being developed which will describe in detail all the principles the SOCIO BEE citizen scientists, recruited during the project will abide by. The Protocol is based on a study of relevant resources (e.g. Hecker (Ed.), 'Citizen Science - Innovation in Open Science, Society and Policy' (2018)) and in line with the 10 ECSA Principles of Citizen Science.[61] This requirement should be fulfilled by M06 and in any case before the recruitment of citizen scientists starts. The citizen scientists will have to be briefed upon the Protocol and agree that they fully understand the principles included in it. Particular attention will be given in the case of children and elderly persons, with the inclusion of specific clauses. That's why the aim of the protocol is to be written in plain and inclusive language and to translate the vision of the project into a "charter" of principles for the participant citizen scientists.

The protocol may be further updated, after it is actually provided to the first participant citizen scientists (for instance, if something is not clear enough or a clause needs to be added) in the next editions of the deliverable, with a clear indication of the change and the reasoning.

[60] SOCIO-BEE D1.4 – Project Handbook, p. 29

[61] ECSA (European Citizen Science Association). 2015. *Ten Principles of Citizen Science*. Berlin. [Online]. Available: http://doi.org/10.17605/OSF.IO/XPR2N

The latest version of this protocol is attached (ANNEX VI). The protocol can also be found at the project's repository on NextCloud.

3.4.5.2 Input from partners

In order to properly implement the above SOCIO-BEE's Ethical Commitment Strategy, all partners in the project were contacted early on (from mid-December). The basis was extensive e-mail exchanges where the necessary data security and ethics documents were exchanged and where there was room for questions and discussion on these issues. Subsequently, bilateral meetings were held with the different partners in the project to get a better understanding of the roles of everyone to not only gather input for D1.5 - Data Management Plan, but also to resolve new questions and establish clear communication between VUB-LSTS and the rest of the consortium. D1.5 is a complex, iterative, multi-level result that will have three versions throughout the project, being this D1.6 its second iteration. Therefore, it is important to contact partners as early as possible. All activities will be closely monitored throughout the project and the partners will take the necessary steps for both data security and ethical requirements.

3.4.5.2.1 Ethics continuous oversight

3.4.5.2.1.1 Current situation

For the previous D1.5 - Ethics Management Plan, several documents were requested and collected where applicable and/or available. In the "Table 4. Overview required documents for D1.5 from the partners in SOCIO-BEE" the situation of each requirement is indicated. Specifically, regarding the ethics input, some partners are not able to provide templates for information sheets and informed consent regarding citizens' participation in research. Others already have their own internally approved templates.

At that early stage in the project, the consortium was working towards clarifying the research design and each partner's specific role in it. Therefore, meetings and workshops were held (in WP2, among others) to get a better overview of how drones, wearables and sensors will be used in SOCIO-BEE and who will take on what role. VUB also participated in those workshops and provided post-meeting a set of points with respect to legal and ethical matters identified during the discussions.

In order to facilitate the process, VUB also hosted several exploratory meetings with partners and also created templates regarding (information sheets and informed consent forms for participation in research and processing of personal data, data protection notice template for the website, data protection policy template for the partners who do not have an explicit policy) which serve as guidelines for those partners in need of such documentation. This way, they are supported to create their own customized versions and check whether their own existing versions meet the requirements of the project. More tailor-made templates will be provided as the project progresses, depending on the needs of the partners.

Another important issue related to the necessary ethical requirements is the process of ethical approvals related to the three pilots of SOCIO-BEE. In SOCIO-BEE, the three pilots will take place in Ancona, Amaroussion and Zaragoza. As these are three municipalities, they do not have an ethics committee. Therefore, CERTH will apply to its ethics committee for these three pilot sites as project coordinator. This includes approvals for research with human participants and the use of wearables and drones. This process is currently ongoing at CERTH. This ethics application will also include information with respect to envisaged rewards or compensation directed towards the participant citizen scientists.

Other partners, such as AUTH, VUB and UDEUSTO are also in the process of establishing the need for further ethical approvals. All the necessary ethical approvals will have to be obtained before the engagement of participants in the project for research purposes.

Lastly, VUB has established a Legal and Ethical documentation repository in the project's common sharing platform, where all documentation provided by the partners (except confidential documents) is stored and remains readily available. Partners have indicated which documentation cannot be provided due to confidentiality reasons and they keep it locally.

As an outcome of T3.1 but with direct relevance to the present evaluation, a Live Glossary of Legal and Ethical (and more) terms was also established, to bridge the communication between the partners coming from different disciplines. The Glossary has been welcomed by the consortium and there are ideas for its further expansion.

The latest versions of these templates are attached (ANNEX VI).

3.4.5.3 The Accord Toolbox

The Accord Toolbox was developed by PRO-RES, a European Commission-funded project, and its use is to assess the ethical quality of research evidence.[62] In SOCIO-BEE, all research studies will follow the respective structure suggested by PRO-RES. Answers to the questions below will be included in future editions of D1.5 as soon as more information is available for each study. The questions are as follows:

- Who will do the research/conducted the enquiry/provided analysis or advice?
- How will they do the research or what will they base their advice and analysis on?
- Whom/what will be studied?
- Why will the research/analysis be conducted?
- When / where will the research/analysis be conducted?
- Will the research be reviewed in advance for quality considerations?
- What will the outcomes be of the research/analysis?

4 Conclusions and Outlook

4.1 Conclusions

D1.6 is a complex, multi-level living document, that requires a high degree of coordination and cooperation among all partners, interacting with many other deliverables and work done within the consortium. D1.6 will be updated as the implementation of the project progresses and when significant changes occur. This is the second of three versions of the Data Management Plan within the framework of the SOCIO-BEE project. This deliverable included two main parts.

The first part included an analysis of the main elements of the data management policy to be used concerning the project. First, a summary was made of the various data that the project will generate. The deliverable identified several data sources that will be analysed, namely: from wearables, drones, sensors, mobile/web applications, questionnaires and surveys, and existing databases. The expected data to be

[62] PRO-RES, 'Accord and Toolbox', [Online]. Available: https://prores-project.eu/accord-and-toolbox/

used and generated during the project is currently categorized in 10 datasets and therefore organized in 10 different factsheets. Moreover, a detailed description of each dataset that are used in the project is provided. These datasets were collected through input from the various partners who will be working on them: CERTH, HYP, UDEUSTO.

This was followed by a discussion on the various aspects of making data from SOCIO-BEE findable, accessible, interoperable, and reusable (FAIR). To help partners with this section, best practices and guidelines have also been added.

In addition, through meetings and extensive e-mail exchanges with the rest of the consortium, input was obtained regarding various legal and ethical requirements necessary for personal and data security in SOCIO-BEE. The partners that need to obtain ethical approvals got this done before the pilots started. Most partners were in order with the remaining requirements. To assist the consortium, a variety of templates are also provided to serve as guides.

The second part consisted of an Ethical Management Plan that implemented SOCIO-BEE's Ethics Commitments Strategy as agreed in the G.A. Guidelines for good and ethical research were also cited by looking at the context in the European Union and the Member States in which the partners are present.

SOCIO-BEE also uses citizen science as a methodology that is difficult to place within the traditional research steps. That is why the ethical implications of citizen science were also considered.

4.2 Future work in next versions

In the last subsequent DMP versions, final information will be available for both parts. D1.6 provides for continuous monitoring of ethics. For example, from the questions in the Accord Toolbox, an interactive diagram will emerge for assessing the ethical quality of research material. Any ethical issues or challenges that may arise will also be closely monitored and considered as input for the next D1.7 versions.

References

[1] ALLEA ALL European Academies (2017). 'The European Code of Conduct for Research Integrity Revised Edition'. Berlin: All European Academies; 2017, [Online]. Available: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf

[2] Berti Suman, A., & Pierce, R. (2018). Challenges for citizen science and the EU open science agenda under the GDPR. European Data Protection Law Review, 4(3), 284-295. doi:10.21552/edpl/2018/3/7

[3] Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648

[4] CESSDA, [Online]. Available: https://www.cessda.eu/Training/Training-Resources/Library/Data-Management-Expert-Guide/5.-Protect/Anonymisation

[5] ENISA, 'Guidelines for SMEs on the security of personal data', [Online']. Available: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[6] ENISA, 'On-line tool for the security of personal data processing', [Online]. Available: https://www.enisa.europa.eu/risk-level-tool/

[7] ENISA, 'Security Measures', [Online]. Available: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/security-measures)

[8] European Commission, 'Ethics and Data Protection', 2018, [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

[9] European Commission, 'Ethics in Social Science and Humanities', 2018 [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf

[10] European Commission, 'Guidelines on FAIR Data Management in Horizon 2020', 26 July 2016. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[11] European Commission, 'H2020 Programme – Guidelines to the Rules n Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020', [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

[12] European Commission, 'Horizon H2020 Online Manual. Ethics.', [Online]. Available: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

[13] European Commission, 'Open innovation, open science, open to the world - a vision for Europe', [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/open-innovation-open-science-open-world-vision-europe

[14] European Commission, 'Online Manual Funding & Tender Opportunities', [Online]. Available: https://webgate.ec.europa.eu/funding-tenders-opportunities/display/OM/Online+Manual

[15] European Commission Decision C(2020)6320 of 17 September 2020), Work Programme 2018-2020, 16. Science with and for Society, [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-swfs_en.pdf

[16] European Data Protection Board, 'EDPB Documents', [Online]. Available: https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf
[17] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, [Online]. Available: https://www.refworld.org/docid/3ae6b3b70.html
[18] ECSA (European Citizen Science Association). 2015. *Ten Principles of Citizen Science*. Berlin. [Online]. Available: http://doi.org/10.17605/OSF.IO/XPR2N
[19] FASTER: D12.1 - POPD - Requirement No. 2 [DPOs and privacy policies for partners processing personal data], 2020., CO.
[20] Fiske, A., del Savio, L., Prainsack, B., & Buyx, A. (2018). Conceptual and ethical considerations for citizen science in biomedicine. In N. B. Heyen, S. Dickel, & A. Brüninghaus (Eds.), *Personal health science* (pp. 195–217). Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-16428-7_10617 https://doi.org/10.1136/medethics-2018-105253
[21] Forsberg, E.-M., et. al. (2018). Working with Research Integrity—Guidance for Research Performing Organisations: The Bonn PRINTEGER Statement. *Science and Engineering Ethics, 24*, p. 1023-1034. doi:10.1007/s11948-018-0034-4
[22] HBM4EU : D10.1 – Data Management Plan, [Online]. Available: https://www.hbm4eu.eu/wp-content/uploads/2017/08/Deliverable-10.1-Data-Management-Plan-August-2017.pdf
[23] OECD, 'Best Practices for Ensuring Scientific Integrity and Preventing Misconduct', 2007, [Online]. Available: http://www.oecd.org/science/inno/40188303.pdf
[24] PANELFIT: D5.4 - Code of Conduct on Data Protection for Responsible Research and Innovation v3.0, 2021, [Online]. Available : https://www.panelfit.eu/wp-content/uploads/2021/03/Panelfit-Code-of-Conduct-on-Data-Protection-CCDP.pdf
[25] PANELFIT, 'D2.1 - Issues and gaps analysis on informed consent in the context in ICT research and Innovation', 2020, [Online]. Available: https://www.panelfit.eu/wp-content/uploads/2020/11/D21-Issues-and-gaps-analysis-on-informed-consent-in-the-context-in-ICT-research-and-Innovation.pdf
[26] PANELFIT, 'Objectives', [Online]. Available: https://www.panelfit.eu/objectives-outcomes/
[27] PROTEIN: D9.1 – Data Management Plan, CO.
[28] PRO-RES, [Online]. Available: https://prores-project.eu/
[29] PRO-RES, 'Accord and Toolbox', [Online]. Available: https://prores-project.eu/accord-and-toolbox/
[30] PRINTEGER, 'About', [Online]. Available: https://printeger.eu/
[31] PRINTEGER, 'The Bonn PRINTEGER Statement, [Online]. Available: https://printeger.eu/the-bonn-printeger-statement/
[32] Quinn, P. (2021). Research under the GDPR – a level playing field for public and private sector research?. Life Sci Soc Policy, 17(4). doi: https://doi.org/10.1186/s40504-021-00111-z
[33] Rasmussen, L. M., & Cooper, C. (2019a). Citizen science ethics. *Citizen Science: Theory and Practice, 4*(1), 5. https://doi.org/10.5334/cstp.235
[34] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, *OJ L 303, 28.11.2018, p. 59–68*
[35] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for

participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/201, *OJ L 170, 12.5.2021, p. 1–68*

[36] Resnik, D. B. (2019). Citizen scientists as human subjects: Ethical issues. *Citizen Science: Theory and Practice, 4*(1), 11. https://doi.org/10.5334/cstp.150

[37] SOCIO-BEE: D1.4 – Project Handbook, v1.0

[38] SEEDS: D6.1 – Ethical Management Plan, 2021, [Online]. Available: https://seedsmakeathons.com/wp-content/uploads/2021/12/SEEDS-Ethical-Management-Plan-March-2021.pdf

[39] Tauginienė, L., et al. (2021). Ethical Challenges and Dynamic Informed Consent. In: K. Vohland et al. (eds.), *The Science of Citizen Science* (pp. 397–416). Springer, Cham. P. 398-399

Annex I – Dataset template

Fact sheet Dataset 1	
Dataset name	- Name of the dataset
Dataset description	- Generic description for the dataset; What type of information
General security and privacy considerations	- Anonymization / pseudonymization - Confidential data - None? - …
Datatype specific answers	
Datatype name	- Name of the datatype
Data description	- Detailed description of the different kinds of data
Data provider and reference	- Who will collect the data - Reference details (if not now, when in project?)
Purpose of data collection	- What is the purpose of the data collection/generation - What will it do; how will it be used; processed; will it use existing data?
Relation to the project	- Its relation to the objectives / tasks / WPs (activities) of the project
Standards and metadata	- In what format(s) will the data be stored?
Data sharing and access	- Who will it be available to and how will access be granted? ○ Within partner's facility ○ Other partners in project ○ Part of dissemination?
Data archiving and preservation	- How and where will it be persevered

Annex II – Data Protection Notice Template for the website or other activities

[Marked in Yellow = this must be adjusted per partner]

Data Protection Notice

The data processing on the XXX is pursuant to the provision of the EU General Data Protection Regulation (GDPR), and in accordance with the country-specific data protection regime applicable to *XXXX*, headquartered in XXXX (EU Member State). For further information, please check Section 2 of the present data protection policy.

Personal data, as defined by Article 4(1) General Data Protection Regulation (GDPR) include any information relating to an identified or identifiable living natural person. Personal data can be your first name, last name, e-mail address, email format and IP address. Hereinafter, by using the terms "we" and "our"; we refer to the data controller, as member of the XXXX consortium. Hereinafter, by using the terms "you" and "your", we refer to the XX.

1. General information: What is [NAME OF PROJECT]?

XXXX is a research project that has received funding from XXXX under grant agreement no. XXX. The project started on XXX and ends on XXX.

XXX info relevant for the project

The present XXXX is part of the XXX.

2. Contact information of the data controller and of the Data Protection Officer

XXX [Website operator/partner]

The Data Protection Officer at XXXX [Website operator/partner] may be reached at [at least an email address].

In case you have any questions about the processing of your data when using the XXX or your rights as data subject, you can also submit your query via our contact form, with the indication "Data Protection Inquiry".

3. Data processing

e.g. a) When using XXX website

You may access the website without having to disclose any data about your person. Nevertheless, the installed browser on your device sends automatically information to the server of the XXXX website, including information about your browser type and version, as well as the date and time of access, so as to establish a connection and permit your access to the website.

e.g. b) When filing a question via our contact form

We offer the possibility to our website visitors to contact us or register an enquiry by submitting an online form through our website. Submitted queries through the form will be sent to the mailbox of the employees in charge of taking care of your requests and will be stored in their email provider servers. Please notice that your data will be stored for as long as necessary for the fulfillment of the purposes specified (reply to your inquiry) and any statutory requirements.

Our contact form requires the minimum information needed in order to be able to respond back to your request. When registering, you need to enter the following mandatory data, marked as such (e.g. with *). These include:

- First name and surname, and
- Email address

The data processing takes place exclusively at your request and in line with article 6(1)(f) of the GDPR. The submitted message, your full name/nickname and email address are processed based on our legitimate interest to be able to provide you with answer to your request. You may object to the processing, by sending an informal email to the email address mentioned in Section 2 of the present policy, requesting the removal of your respective data.

To secure the website from malicious activity, we use the Securimage-WP CAPTCHA protection to the contact and comment forms of our website. This tool does not use cookies.

c) Leaving comments on our website

When you use the comment function, the time at which you created the comment and your email address will be stored along with your comment and your full name, unless you decide to upload your post by using a nickname. The comments as well as your full name/nickname remain publicly visible on our website for as long as the content commented upon has been completely deleted or the comments are required to be removed, for instance, upon your request or under legal justification. Please note that your data will be stored for as long as necessary for the fulfillment of the purposes specified (public posting of your comments on the XXX website) and any statutory requirements. The submitted comments, your full name/nickname and email address are processed based on your informed consent per Art. 6 (1) (a) GDPR when you click on 'By clicking on the submit button, I agree to the XXX website Data Protection Policy.' You may withdraw your consent at any time with future effect and request the deletion of your post, by sending an informal email to the email address mentioned in Section 2 of the present policy, requesting the removal of your data.

4. Cookies

Cookies are small text files that are automatically placed on your browser and stored on your device when you visit a website. The only cookies used on the XXX website are **first-party cookies (cookies set by the website you are visiting and not third parties)**, placed with the support of MATOMO in order to capture statistical data on the website usage and for security purposes. MATOMO is an open-source analytics platform. It powers the Europa Analytics, the corporate service that monitors and evaluates the effectiveness and efficiency of the European Commission's websites.

XXX retains control of the data collected through those first-party cookies by storing the data in servers controlled by XXX.

The XXX website uses the MATOMO-powered cookies to communicate to the European Commission the efforts we are making to disseminate our research output by providing relevant anonymous statistical data about web visits.

The data collected for those purposes by MATOMO are:

- IP address
- Country

The IP anonymiser feature provided by MATOMO is enabled, making it impossible to identify a particular XXXX website visitor via the sole IP address. The generation of visitor profiles is disabled. MATOMO automatically deletes visitors' logs after 13 months. Anonymized data are stored by the XXX website operators for as long as necessary to fulfil the consortium's contractual obligations and no longer than the project duration.

Cookies strictly necessary for the security and basic function of the website are installed automatically and dot require your consent. Cookies which are not required for the aforementioned reasons, require your explicit consent. Some cookies are deleted automatically after you close your browser. Other cookies, the so-called long-term/persistent cookies, may remain on your device or be automatically deleted after a defined period of time. You can provide or withdraw your consent at any time through the website's cookie banner. The cookie banner is always accessible at the right bottom page of the website, by clicking on XXXX .

The list of cookies on the XXXX website is the following:

Website	Cookies	Purpose
	cookielawinfo-checkbox-necessary	It stores the user's decision on accepting cookies.

If you wish to adapt your settings through our cookie banner

If the *Do Not Track* option is not enabled or if you visit our website for the first time, you will be presented with a cookie banner where you can install a cookie called "cookielawinfo-checkbox-necessary" which will keep track of your choice. If you consent to anonymized analytics, then XXXX.

You can withdraw your consent or decide to consent again at any time through the cookie banner.

If you do not wish to install cookies for anonymized analytics

By default, the browsing experience of our website visitors is not tracked. Moreover, you can in general prevent the storage of cookies, by properly configuring your browser settings, for instance, by choosing the "disable cookies" function or the *Do Not Track* option, by enabling notifications before a new cookie is installed or by using a tool/add-on for cookies management. The XXXX website will respect your choice and your browsing experience on our website will not be tracked for our anonymized statistics.

5. Social media plug-ins

We use social media to present and communicate our work through widely used communications channels, and maximise the impact of our research activities. Thus, on certain webpages of the XXX website, we use social media plug-ins (the so-called social media buttons) to enable this interaction. These plug-ins are small buttons, which can be recognized by bringing a social media logo, for instance the Facebook or Twitter logo. The function of these buttons is to allow you to share the contents of the

XXX website in your profile on social networks, to access via links the XXX accounts in other social platforms, or to watch an embedded (or not) YouTube video of XXX activities. As of XXX, the XXX consortium is active on four social networks: Facebook, Twitter, LinkedIn and YouTube.

The XXX website uses the Shariff solution, which is an open-source, low-maintenance, privacy-preserving tool maintained by the German computer magazine c't and heise online. As long as you do not interact with the social media buttons on the XXX website by clicking on them, personal data of yours are not transmitted to the social media platforms by the mere fact that you are visiting our webpages, where these buttons appear. However, if you click on such a button, a connection is established between the XXX website and the social network. In that case, in addition to the contents in question, the operator of the social network may also obtain additional, partly personal, information, for instance, information about your XXX website visit.

The XXX website does not set cookies when displaying links to our social media channels. Nevertheless, each social media platform has their own data protection policy when accessing their websites. For example, if you choose to read our news on Twitter, you will be asked for explicit consent to accept Twitter cookies, and the same applies for all the other platforms. Moreover, if you do not wish the social media platforms to track data collected about you via our website back to your personal accounts, then please log out of your social media accounts before visiting our website.

Specifically, we use the following social media plug-ins:

Facebook Ireland Limited: share/link button

By clicking on the Facebook icon on our website, you will be re-directed to the Facebook website, which has its own cookie and privacy policies over which we have no control. For more information, please refer to the Facebook privacy notice.

Twitter International Company: share/link button

By clicking on the Twitter icon on our website, you will be re-directed to the Twitter website, which has its own cookie and privacy policies over which we have no control. For more information, please refer to the Twitter privacy statement.

LinkedIn: share/link button

By clicking on the LinkedIn button on our website, you will be redirected to the LinkedIn website, which has its own cookie and privacy policies over which we have no control. For more information, please refer to the LinkedIn privacy statement.

YouTube: link button

At the moment, there are no embedded videos on the XXX website. If, in the future, there will be such embedded videos, we will be using the "extended data protection mode", provided by YouTube. In doing so, access to the XXX website visitors´ personal data by solely loading a webpage containing an embedded YouTube video from the XXXX official YouTube account is prevented. In order to watch a video on our website, a message will alert you that you need to accept YouTube cookies to do so. YouTube has its own cookie and privacy policies over which we have no control. There is no installation of cookies from YouTube until you consent to YouTube cookies and then are redirected to the YouTube website. For more information on data protection with LinkedIn, please refer to the privacy policy of Google.

6. Data Handling, Legal basis and Purpose of the processing

Data Matrix template

Personal data	Processing	Purpose of the processing	Legal basis of the processing	Retention period
e.g. full name	e.g. collection, retrieval, use, evaluation, combination, etc.	e.g. for providing you with information about the research progress as requested by you	e.g. performance of contract, user's consent, public interest	e.g. as long as it is necessary for the processing and no longer than 6 months after the project ends. In case of consent, consent is withdrawn or the data are not necessary anymore for the purpose they were initially collected

7. Your rights as a data subject

As a data subject, you have the following rights:

- pursuant to Article 7(3) GDPR, to **withdraw your consent at any time and without any consequences for you.** This means that in future we may no longer continue to process the data as based on this consent;
- pursuant to Article 15 GDPR, to **obtain information** about whether your personal data are processed by us and where that is the case, access to those personal data. In particular, you may obtain information about the purpose of processing, the category of the personal data, the categories of recipients, to whom your data has been or is disclosed to, the storage period planned, the existence of a right to request from the controller rectification, erasure, restriction of processing or objection, the existence of a right to lodge a complaint and the source of your data if it has not been collected by us. Pursuant to Article 12, we must provide any communication relating to the processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- pursuant to Article 16 GDPR, to **obtain the rectification of inaccurate personal data** without undue delay or the completion of your personal data stored with us;
- pursuant to Article 17 GDPR, to **obtain the erasure of your personal data** stored with us unless processing is necessary to exercise the right to freedom of expression and information, for compliance with a legal obligation, for reasons of public interest, or to establish, exercise or defend legal claims;
- pursuant to Article 18 GDPR, to **obtain the restriction of the processing of your personal data**;
- pursuant to Article 20 GDPR, to **receive your personal data, in a structured, commonly used and machine-readable format** or to obtain the transmission to another data controller (right to data portability);
- pursuant to Article 21 GDPR, to **object**, on grounds relating from your particular situation, at any time to processing of your personal data, which is based on data processing for the purposes of legitimate interests. If you file an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or unless processing serves the establishment, exercise or defence of legal claims.

If you wish to exercise your rights or you wish to receive more information, please go to Section 2 - Contact information of the data controller and the Data Protection Officer, where you can find the most updated contact information.

Pursuant to Article 77 GDPR, you also have the right to **lodge a complaint** with a national supervisory authority. You can contact the supervisory authority of your habitual residence or workplace or of our company headquarters. In the latter case, you can file a complaint with the XXXX [Name of national data protection authority].

8. Data security

Moreover, we use suitable technical and organizational measures, which are being continuously enhanced, to protect your data against accidental or intentional manipulation, partial or complete loss, destruction or against unauthorized access by third parties.

9. Amendments to this Data Protection Policy

This data protection policy is effective as of XXXX. The policy was reviewed and amended in XXX.

We keep our Data Protection Policy under regular review to make sure it is up to date and precise. Thus, it may become necessary to change it due to the potential addition of new features to the XXX or due to further legal requirements.

Annex III – Data Protection Policy Template

The template provided below is to be implemented and detailed by project's partners processing personal data with regards to their activities in SOCIO-BEE and not appointing DPO. This template for the Data Protection Policy was taken from the FASTER project, D12.2 - POPD - Requirement No. 2 [Partners' DPOs and form of privacy policy], and adapted for SOCIO-BEE.

[BEGINNING OF THE FORM]

1. Introduction
   1.1. This document represents the policy of [**partner's name**] (hereinafter – **'we'/'us'/'Organization'**) with regards to the processing of personal data within the SOCIO-BEE project.
   1.2. SOCIO-BEE project (Wearables and droneS fOr CIty Socio-Environmental Observations and BEhavioral ChangE) is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. 101037648.
   1.3. The overall aim of the SOCIO-BEE project is to develop low-cost technological innovations and instruments that will tangibly contribute to the overall pro-climate campaign, with primary focus on improving air-quality in urban areas.

2. Scope of the policy
   2.1. This policy only considers the processing of personal data by the Organization concerning its participation in the SOCIO-BEE project. Other processing activities carried out by the Organization are outside the scope of this policy.
   2.2. The participation of the Organization in the SOCIO-BEE project will include [the type and description of activities, pilots where the Organization is involved, other relevant details].
   2.3. The Organization's activities in SOCIO-BEE will include the following processing of personal data: [types of personal data and data subjects, processing activities, and purpose(s) of processing].
   2.4. The legal basis for processing personal data is explicit and informed consent of data subject. We use the template developed for SOCIO-BEE's partners and specified in the D1.5.

3. Data protection principles
   We support the principles set out by the GDPR by the following measures:
   3.1. **lawfulness, fairness, and transparency of processing**: we process personal data on the basis of informed and explicit consents of data subjects; provide them information sheets describing the processing activities, explain the relevant information about the project and processing process through communication with a data subject;
   3.2. **purpose limitation**: we only process personal data that is necessary to reach the goals of the project;
   3.3. **data minimization**: we only collect and process personal data that is strictly necessary to conduct our activities in SOCIO-BEE;
   3.4. **accuracy of data**: we update/modify/erase the data upon request of the data subject or upon other discovery of its incorrectness;
   3.5. **storage limitation**: we store the data during the term of the project and for [term] after its finishing; we irrevocably delete the data or anonymize it after the end of its processing;
   3.6. **integrity and confidentiality**: we limit the scope of people having access to personal data to those who work in our Organization and participate in the project; we store the

personal data separately and use authentication procedures to control the access to it; [other applicable security measures to be added];

3.7. **accountability**: we use this policy to set and demonstrate compliance with the GDPR [other ways to be compliant and demonstrate it if necessary].

4. Rights of data subjects

We respect the rights of data subjects specified in the GDPR, including:

4.1. the right to ask us what data are being collected about the data subject and how those data will be used in connection with the SOCIO-BEE project ("right to access");

4.2. the right to lodge a complaint with a supervisory authority ("right to complain");

4.3. the right to request us to correct any of data subject's personal data that are inaccurate ("right to rectification");

4.4. the right to request us to erase data subject's personal data ("right to erasure" also "right to be forgotten"), unless such a request would render impossible or seriously impair the achievement of the objective of that processing – including the impairment or invalidation of the research;

4.5. the right to request us to restrict the processing of data subject's personal data ("right to restriction of processing");

4.6. the right to receive the personal data related to the data subject which he/she has provided to us and to transmit those data to another controller ("right to portability"); and

4.7. the right to object, at any time, to us regarding the processing of data subject's personal data ("right to object").

5. Other provisions

5.1. This policy is effective as of [date] till the end of the processing activities [the period after the end of the SOCIO-BEE project to be defined].

5.2. This policy will be reviewed annually and updated if needed until the end of its effect.

5.3. We have chosen not to appoint the Data Protection Officer while it is not required for our processing activities.

5.4. All our employees having access to personal data specified herein, will be informed on this policy and other measures expected from them to be compliant with the GDPR.

5.5. The person controlling the implementation of this policy and other measures to comply with the GDPR from the side of the Organization is [name and contact details of the Organization's employee representing SOCIO-BEE].

[END OF THE FORM]

Annex IV – Data Security Protocol

Acknowledgement: This summary is based on "Data Security Procedures for Researchers" (J-PAL NA, 2018). This draft version will be further complemented in the next versions of the DMP.

Data security overview

It is crucial that researchers treat data security seriously as it's critical to protecting data, respecting the privacy of research subjects, and complying with applicable protocols and requirements.

Data security breaches: causes and consequences

A data security breach can result in serious consequences for research subjects, the researcher's home institution / company / organization, and the researcher. Sensitive data are especially vulnerable to both inadvertent disclosure and targeted attacks.

Minimizing data security threats

Reduce the data security threat-level a priori by acquiring and handling only the minimum amount of sensitive data strictly needed for the research study.

Deidentifying data

Separate Personally Identifiable Information (PII) from all other data as soon as possible. Data pose the most risk when sensitive or confidential information is linked directly to identifiable individuals. Once separated, the "identifiers" data set and the "analysis" data set should be stored separately, analyzed separately, and transmitted separately. Once separated, the identifiers should remain encrypted at all times, and the two data sets should only meet again if necessary to adjust the data matching technique. In order to maintain the ability to re-identify the analysis data set, a unique "Study ID" can be created by the researcher, data provider, or implementing partner. This ID should be created by a random process, such as a numbered list after sorting the data on a random number, or through a random number generator.

Data storage & access

Researchers have many options for secure data storage and access. Relevant considerations for choosing among these options include: the sensitivity of the data, applicable compliance requirements, the research team's technical expertise, internet connectivity, and access to IT expertise and support.

Encryption

Encryption is the conversion of data to code that requires a password or pair of "keys" to decode. Data may be encrypted at many levels, at multiple stages of the data lifecycle, and through a variety of software and hardware packages.

- *Device-level (whole-disk) encryption*: Computers, flash drives, tablets, mobile phones, and any other hardware for data storage and/or primary data collection may be whole-disk encrypted. This method protects all files on the device, and requires a password upon device start-up
- *Cloud storage*: Without a formal agreement to store data in compliance with a specific set of regulations or other file-level encryption, simply storing files using these services is not a fully secure option for sensitive data. The original data provider and any reviewing IRBs should be consulted prior to initiating agreements with cloud-storage providers.

- *Folder-level encryption:* While cloud storage tools encrypt the connection and files "at rest" on their systems, they retain the encryption keys, which technically gives their employees read access to all files saved on their servers. To address this, tools including Boxcryptor and VeraCrypt encrypt files before they are stored in the cloud. Boxcryptor is a paid subscription model, whereas VeraCrypt is free and open-source
- *File-level encryption:* While whole-disk or device-level encryption encrypts all files on a device, it does not protect the files once they leave the device--for example, while they are in transit or being shared with another researcher. File-level encryption applies to specific files, and facilitates data sharing. Proper use of file-level encryption requires strong protocols for password sharing and for unlocking and relocking files before and after use. Options for file-level encryption include PGP-Zip and 7-zip.
- *IT-administered options:* For researchers with access to a professional IT team, and whose team members have access to reliable, fast internet, IT-administered options may be preferable. These options allow researchers to delegate the administration of a data access and storage solution to IT experts. IT administrators may also be able to provide several additional levels of data protection. As with cloud storage, IT staff may have access to all data on a server, including Personally Identifiable Information. Researchers should be sure to understand who has access to the data, and maintain as much direct control as possible to prevent compliance issues or accidental data breaches.

Data transmission and sharing

Data must be protected both when at rest and in transit between the data provider, research team members, and partners. Data that are encrypted while at rest on a whole-disk encrypted laptop, or on a secure server, will not necessarily be protected while being transmitted. The options presented below may vary in their level of security.

Communication and data sharing with partners

It is best practice to develop a data sharing and security protocol with all the partners, and to guide them in understanding their role in data security. All partners handling or transmitting data should be informed of and trained on data collection, storage, and transfer policies agreed upon for the study. Request that partners notify the research team before sharing any data to ensure compliance with the data protocol. Teams should communicate with each other and with partners by referencing Study ID numbers rather than using PII. Consider developing standard operating procedures for checking for and responding to breaches in following the agreed upon method for sharing data. For example, if partners share data in a non-secure way or if unauthorized data are disclosed to researchers or partners. This will allow staff to respond quickly in the event of a breach. A standard operating procedures document should include:

1. Process for sharing data and receiving updates
2. Process for verifying data set does not contain unauthorized information prior to downloading, if possible
3. Timeline for reviewing new data for unauthorized information or PII
4. Plan for notifying the source of the breach and requesting corrective action to prevent future breaches
5. How files with unauthorized information will be removed and destroyed

These standard operating procedures are discussed in D1.5 and will be further supplemented throughout the project.

Personal device security

There are several simple steps researchers and their staff can take to ensure their machines remain secure and to minimize possible weak points. These steps include:

- Keep all software up to date. Most computers and platforms regularly check for new versions of software. New versions are often created to fix security problems or other known issues.
- Use data repositories hosted in secure infrastructures

Password policies

Strong passwords are essential to ensuring data security. A different password should be used for each high-value account. For example, the passwords for Dropbox, email, institutional servers, and encrypted files should all be different.

- *Do not forget your password*: Strong passwords may be difficult to remember. When using some software, such as Boxcryptor, a forgotten password is completely irretrievable and means the loss of all project data.
- *Store and share passwords securely*: An unencrypted, password-protected Excel file of passwords is not a secure way to store or share passwords. Passwords should never be shared using the same mechanism as file transfer, nor should they be shared over the phone.

Preventing data loss

In addition to securing against outside threats, preventing data loss is an essential component of data security. Data and crosswalks between study IDs and PII should be backed up regularly in at least two separate locations, and passwords must not be forgotten.

Erasing data

The data provider may dictate whether and when data must be retained or destroyed. PII linkages should be erased when they are no longer needed. Simply moving files to the “recycle bin” and emptying the bin is not sufficient to thoroughly erase sensitive data.

ENISA and GDPR security measurements

GDPR

The GDPR stipulates in Art. 5 the principle of security (integrity and confidentiality) in addition to the other GDPR principles such as lawfulness, fairness, etc. To this end the GDPR also falls under the 'common information security and information security management' which stipulates a risk-based approach. In addition, it also provides additional security for personal data in Art. 32 GDPR.

“Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organizational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate: (a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. The article further stipulates that in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed’. It also mentions that adherence to an approved code of conduct (Article 40 GDPR) or an approved certification mechanism (Article 41 GDPR) may be used as an element to demonstrate compliance with the requirements for the security of processing. Last, it states that the controller and processor ‘shall take steps to ensure that any person acting under their authority and having access to personal data, shall not process them except on instructions from the controller, unless otherwise required by Union or member state law”. [63]

Based on the aforementioned provisions, there are a number of important observations that should be made with regard to the security of personal data under GDPR:

- **Risk-based approach**: Technical and organizational measures for the protection of personal data should, according to GDPR, be appropriate to the risk presented.
- **An information management system for personal data**: The GDPR provision goes beyond the mere adoption of specific security measures, supporting the establishment of a thorough information management system for the protection of confidentiality, integrity, availability and resilience of personal data.
- **Security for privacy**: Although GDPR does not provide a direct reference to privacy enhancing technologies (PETs)27, it specifically addresses pseudonymization and encryption as core protection measures for the security of personal data.

[63] GDPR, art. 32; ENISA, ‘Guidelines for SMEs on the security of personal data’, [Online’]. Available: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing, p. 12-13

Guidelines ENISA[64]

ENISA has released several publications that can support organizations and especially SMEs in taking the appropriate technical and organizational security measures regarding personal data when acting either as data controllers or data processors (under GDPR): [65]

Guidelines for SMEs on the security of personal data

"In complying with the GDPR obligations, ENISA proposed a risk-based approach for the adoption of security measures for the protection of personal data, namely: Guidelines for SMEs on the security of personal data processing". This guideline includes a step-by-step guide for assessing security risks for personal data. "It presents a simplified approach that can guide the SMEs through their specific data processing operation and help them evaluate the relevant security risks. As such, the proposed approach does not present a new risk assessment methodology but rather builds on existing work in the field to provide guidance to SMEs (…). It should be noted that the work is focused solely on security risk assessment and should not be confused with data protection impact assessment (DPIA - Article 35 GDPR). While the former is a critical part of the latter, a DPIA takes into account several other parameters that are related to the processing of personal data and go beyond security. Still, the proposed approach could also be useful in the context of a DPIA and/or could be extended in the future to also cover DPIA conduction".[66]

The proposed approach is based on four steps, as follows[67]

1. Definition of the processing operation and its context;
2. Understanding and evaluation of impact;
3. Definition of possible threats and evaluation of their likelihood (threat occurrence probability);
4. Evaluation of risk (combining threat occurrence probability and impact).

Online tool

ENISA has also provided an online tool for the security of personal data processing to assist in the practical implementation of the previous guide.[68]

[64] The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe
[65] ENISA, 'Security Measures', [Online]. Available: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/security-measures)
[66] ENISA, 'Guidelines for SMEs on the security of personal data', [Online']. Available: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing , p. 17
[67] Ibid.
[68] ENISA, 'On-line tool for the security of personal data processing', [Online]. Available: https://www.enisa.europa.eu/risk-level-tool/

Annex V – Template Joint Controllership Agreement

Acknowledgement: This template is based on various templates such as "Template for Joint Controller Agreement of collaboration" (ERA LEARN, 2021); "Model Joint Controllership Agreement" (SURF, 2019); "Model Joint Controllership Agreement" (SURF, 2019).

Template for Joint Controllership Agreement

THIS JOINT CONTROLLER AGREEMENT is made on {date}, hereinafter referred to as the 'Effective Date'

BETWEEN:

1. **xxx,** established in {address}, the Coordinator of the consortium, and
2. **…**
3. **…**

hereinafter, jointly or individually, referred to as "Joint Controllers" or "Parties" relating to the project entitled

{Name of Programme}, in short: **xxx**, hereinafter referred to as 'Programme'.

Whereas:

A. pursuant to the Consortium Agreement of [date] , (hereinafter referred to as the "Consortium Agreement") and the Grant Agreement of [date] no. ... signed between the European Commission and the [name of Programme] consortium, the Joint Controllers have entered into cooperation the subject of which is to conduct a joint call for proposals and perform additional activities within a consortium of executive agencies (hereinafter referred to as the "Cooperation");

B. the Cooperation requires that the Joint Controllers process personal data, whilst they jointly determine the purposes and means of processing of personal data;

C. the processing of personal data by the Joint Controllers requires that a transparent manner of determining their respective responsibilities be established as regards their compliance with the obligations under the 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 (hereinafter referred to as "General Data Protection Regulation" or "the GDPR"[69]) and other generally applicable laws as well as relations between the Joint Controllers and the data subjects;

D. on concluding this Agreement, the Parties, seek to regulate the terms of processing of personal data in such a way that they meet the provisions of the GDPR, and

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

E. with regard to the data they process, the Joint Controllers act as controllers for the purposes of Article 24 et seq. of the GDPR referred to in D,

the Parties decided to enter into the following Agreement:

§ 1.

Definitions

For the purposes of this Agreement, the Parties agree that the following definitions and terms shall have the following meaning as defined in the GDPR:

1. **"Controller/Joint Controller"** means any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
2. **"Personal Data"** means any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject");
3. **"Third Country"** means any country that is not a member of the European Union or the European Economic Area or any international organization;
4. **"Processor"** means any natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller;
5. **"Data Protection Law"** means the GDPR as well as other provisions of EU Member State's national law applicable to a relevant Party, passed in relation to personal data protection, including in particular the provisions of the given Controller's national law;
6. **"Processing**" means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
7. **"General Data Protection Regulation"**, **"GDPR"** means the 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; wherever this Agreement refers to specific Articles of GDPR, it shall also apply to the corresponding provisions in national legislation guaranteeing a similar level of safety;
8. **"Information System"** means a group of cooperating devices, programs, information processing procedures and program tools used for the purpose of data processing;
9. **"Cooperation"** means the cooperation between Controllers defined in Recital A;
10. **"Agreement"** means this Agreement on Joint Control of Personal Data;
11. **"Consortium Agreement"** means the agreement referred to in Recital A

§ 2.

Subject-matter of the agreement

1. This Agreement regulates mutual relations between the Parties as regards the joint control of Personal Data, and in particular it determines in a transparent manner the Joint Controllers' responsibilities for compliance with the obligations under the GDPR; it also defines the

representation of the Joint Controllers in contacts with the data subjects and their relations with those data subjects.

2. For the purpose of proper implementation of this Agreement, the Joint Controllers shall:
   1) cooperate on performing the obligations of the Joint Controllers of Personal Data;
   2) process the Personal Data with which they have been entrusted with regard to the Cooperation pursuant to this Agreement, GDPR, Consortium Agreement and other generally applicable laws and
   3) refrain from any legal or factual actions which might in any way undermine the security of Personal Data or threaten the other Joint Controller with civil, administrative or criminal liability.
3. Categories of data subjects and personal data, the purposes and means of processing, including the participation of Joint Controllers in those processes, as well as the categories of recipients of the Personal Data shall be defined in Appendix 1 to the Agreement.[70]

§ 3.

Controllers' rights and obligations

1. The Joint Controllers declare that they have the means enabling them to process and protect Personal Data they are processing, including information systems meeting the requirements of the appropriate level of security, as stipulated by the GDPR. They will each fully adhere to the applicable Data Protection Law(s) with respect to obligations and responsibilities of controllers.
2. In particular, the Joint Controllers shall:
   1) exercise due diligence in processing Personal Data and process Personal Data pursuant to the Agreement, the GDPR and other provisions of Data Protection Law(s), including the appropriate provisions of each Controller's national law;
   2) restrict access to Personal Data only to persons who need the access to Personal Data for the purposes of the Agreement and Cooperation, provide those persons with relevant authorisations, offer relevant training on personal data protection and ensure confidentiality of Personal Data processed thereby, both during and after their employment or other cooperation with a Joint Controller;
   3) assist the other Joint Controller, where possible, in meeting its (i) obligation to respond to requests from data subjects and (ii) obligations laid down in Articles 32 through 36 of the GDPR;
3. The Joint Controllers shall provide each other with the necessary assistance in carrying out the obligations referred to in section 2 point 5) above, in particular in the notification of a personal data breach, by:
   1) providing, at the request of a Controller, information concerning the processing of personal data immediately upon receipt of such request as soon as possible;

[70] The appendices mentioned throughout the text include Appendix 1: essential elements of the means and Appendix 2: Information to be provided to the data subjects. Both appendices will be drafted to serve the purpose of the agreement.

2) notifying the other Joint Controllers of any breach as soon as possible but not later than 48 hours of its discovery. The notification should include all the information referred to in Article 33 (3) of the GDPR. If - and to the extent that - the information cannot be provided at the same time, they can be given successively without undue delay;

3) providing to the other Joint Controllers all information necessary for the communication of a personal data breach to the data subject;

4) informing the other Joint Controllers of inquiries, requests or demands from data subjects and other individuals, national or European Union public administrations, including relevant supervisory authorities and courts, as well as any controls or inspections by such authorities in connection with the joint controllership of Personal Data; information shall be provided promptly and in such a way as to enable the other Joint Controllers to comply with the obligations set out in sections 2 and 3, without undue delay but not later than 7 calendar days after receipt of an inquiry, request or demand or after the start of a control or inspection.

§ 4.

Data subjects' rights

1. The Joint Controllers shall inform, in any way they deem appropriate, the data subjects of the essences of this Agreement and shall provide them the information referred to in Appendices 1 and 2 in accordance with Article 26 and Article 12 of the GDPR.
2. The information referred to in section 1 shall be primarily provided to the data subjects via the electronic proposal submission system or by the Controller who collects the personal data.
3. Data subjects may contact any of the Joint Controllers about the rights granted to them by Articles 15 - 22 of the GDPR. The contacted Controller shall identify the responsible Controller and forward the request internally to this Controller. The originally contacted Controller shall carry out all necessary communication with the data subject.
4. The responsible Controller shall be determined as follows: If the data of the data subject is part of a set of data which can be attributed to a Controller, this Controller shall be responsible. In all other cases the Controller contacted by the data subject shall be the responsible Controller.
5. The Joint Controllers undertake to comply with the data subjects' rights and shall assist one another with the execution of data subjects' requests.

§ 5.

Transfers of Personal Data to third countries

Controller and/or its Processor(s) that transfer(s) personal data in the scope of the execution of the Agreement to a Controller and/or Processor and/or other entity situated in the third country that does not present adequate safeguards under the GDPR shall ensure that such transfer is possible and that it complies with the GDPR (e.g. pursuant to Article 45 of the GDPR – on the basis of an adequacy decision Article 46.2.c) of GDPR – on the basis of standard data protection clauses adopted by the Commission in accordance with the examination procedure in Article 93.2 or pursuant to Article 49 of the GDPR. A copy of standard data protection clauses referred to in the preceding sentence shall be provided when so requested by a data subject.

§ 6.

Entrusting Processors with processing of Personal Data

1. The Controllers jointly consent to each of them entrusting Processors with processing of Personal Data subject to this Agreement on terms and to the degree defined by this Agreement and Article 28 of the GDPR.
2. Each Controller may entrust Processors with processing of Personal Data under this Agreement only for the purposes of this Agreement, Consortium Agreement and the Cooperation.
3. Processors can only carry out specific Personal Data processing activities on behalf of a Controller once the Controller has entered into a contract with such a Processor laying down the obligations of the latter related to Personal Data protection in a manner ensuring sufficient guarantees of technical and organizational measures for the processing to meet the requirements of the GDPR.
4. A Processor may carry out specific Personal Data processing activities on behalf of a Controller without entering into the contract referred to in section 3 as long as it is possible pursuant to another legal instrument under EU law or national law, which binds the Processor and the Controller.
5. This Paragraph shall apply in the case of any intended modifications regarding adding processors or replacing processors with other processors.
6. Categories of processors are listed in Appendix 1. The Joint Controller shall provide detailed information on its Processors on request to the data subject

§ 7.

Controllers' liability

The liability of the parties is governed by the legal regulations, in particular Article 82 of the GDPR with regard to the processing activities that they are in charge of as defined in regard of the Controller's role in the Collaboration and as stated in Appendix 1

§ 8.

Collaboration of the Parties

1. The Parties shall cooperate in supervising the implementation of this Agreement.
2. The Parties agree that at the time of the implementation of the Agreement they shall cooperate closely, informing one another of any circumstances that have or may have effect on processing of Personal Data.
3. Each Party designates a contact point to coordinate the collaboration of the Parties in connection with the implementation of the Agreement, disclosing their personal data in point 1 of the Appendix 2.
4. Amendments to Appendices 1 or 2 shall not require an amendment of the Agreement, however all Parties shall have to be notified thereof either in writing or electronically by the Coordinator.

§ 9.

Term and termination of the Agreement

1. The Agreement will take effect as of the Effective Date.
2. This Agreement can only be amended by the Parties following a consultation of all participating Parties, and provided that all participating Parties have agreed to the proposed amendment. If applicable law and regulations are amended, the Parties shall seek to amend this Agreement accordingly.
3. The Agreement shall be concluded for the period of implementation of the Cooperation and as long as and until, after the termination of the Cooperation, obligations still have to be fulfilled.

§ 10.

Final provisions

1. The Parties hereby agree that the Controllers shall process Personal Data pursuant to this Agreement free of charge, and neither the conclusion of this Agreement nor the processing of data pursuant thereto shall entitle any Controller to seek, on whatever legal basis,
    1) remuneration,
    2) reimbursement of any costs or expenses incurred for the purpose of due performance of the Agreement,
    3) exemption from any obligations contracted to that end or advances on such costs or expenses,

   even if at the time of entering into Cooperation or concluding this Agreement, despite exercising due care, the Controller was unable to foresee the circumstances justifying such rises, costs, expenses or obligations.
2. Should any provision hereof become invalid or ineffective, the Parties shall adopt all measures possible to replace it with a valid and effective provision reflecting the goal and meaning of the invalid or ineffective provision to the extent of applicable law. Should any provision hereof be or become invalid or ineffective at any time, it shall not restrict the validity or effectiveness of the remaining provisions of the Agreement.
3. In the event of any discrepancies between the provisions of the Agreement and the terms of Cooperation agreed by the Parties, the provisions of this Agreement shall prevail.
4. Any amendments hereto must be in writing on sanction of invalidity, subject to § 8 (4).
5. Any disputes arising under the Agreement shall be resolved by amicably or by a common court with jurisdiction over the registered office of the Controller sued and pursuant to the laws applicable in its country.

This Agreement has been drawn up in … counterparts, one counterpart for each Party.
Signatures of the Parties (in the case of a multilateral agreement, each Controller on a separate page):

Annex VI - Executed Joint Controllership Agreement

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement n° 101037648 – SOCIO-BEE

Grant Agreement No: 101037648
[H2020-LC-GD-2020-3]

Wearables and droneS fOr CIty Socio-Environmental Observations and Behavioral ChangE

Joint Controllership Arrangement

Joint Controller Arrangement

THIS JOINT CONTROLLER ARRANGEMENT is made on April 30 2023, hereinafter referred to as the 'Effective Date'

BETWEEN:

1. ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (CERTH), established in CHARILAOU THERMI ROAD 6 KM, THERMI THESSALONIKI 57001, Greece, VAT number: EL099785242, *the Coordinator of the consortium*, and
2. ARISTOTELIO PANEPISTIMIO THESSALONIKIS (AUTH), established in KEDEA BUILDING, TRITIS SEPTEMVRIOU, ARISTOTLE UNIV CAMPUS, THESSALONIKI 54636, Greece, and
3. BETTAIR CITIES SL (BETTAIR), established in TRAVESSIA INDUSTRIAL 149 4C, HOSPITALET DE LLOBREGAT 08907, Spain, and
4. NILU STIFTELSEN NORSK INSTITUTT FORLUFTFORSKNING (NILU), established in INSTITUTTVEIEN 18, KJELLER 2027, Norway, and
5. UNIVERSIDAD DE LA IGLESIA DE DEUSTO ENTIDAD RELIGIOSA (UDEUSTO), established in AVENIDA DE LAS UNIVERSIDADES 24, BILBAO 48007, Spain, and
6. UNIVERSITA POLITECNICA DELLE MARCHE (UNIVPM), established in PIAZZA ROMA 22, ANCONA 60121, Italy, and
7. HOP UBIQUITOUS SL (HOPU), established in CALLE LUIS BUNUEL 6, CEUTI 30562, Spain, and
8. FUNDACION IBERCIVIS (IBER), established in CALLE MARIANO ESQUILLOR SN CAMPUS RIO EBRO EDIFICIO I+D BLOQUE 2 PLANTA 2, ZARAGOZA 50018, Spain, and
9. FUNDACION ZARAGOZA CIUDAD DE CONOCIMIENTO (ZKF), established in AVENIDA CIUDAD DE SORIA 8 EDIFICIO E2 PLANTA 6 DENTRO DEL ETOPIA, ZARAGOZA 50003, Spain, and
10. AYUNTAMIENTO DE ZARAGOZA (ZGZ), established in PLAZA DEL PILAR 18, ZARAGOZA 50071, Spain, and
11. MUNICIPALITY OF AMAROUSSION (MRSI), established in 9 VASILISSIS SOFIAS STR AND D. MOSCHA STR., AMAROUSSION 15124, Greece, and
12. COMUNE DI ANCONA (ANCONA), established in PIAZZA XXIV MAGGIO 1, ANCONA 60124, Italy.

hereinafter, jointly or individually, referred to as "Joint Controllers" or "Parties" relating to the project entitled **SOCIO-BEE**, funded by the European Commission under the Grant Agreement No. 101037648, hereinafter referred to as 'Project'.

Whereas:

A. pursuant to the Consortium Agreement dated September 2021, (hereinafter referred to as the "Consortium Agreement") and the Grant Agreement no. 101037648 dated 31 August 2021 signed between the European Commission and the SOCIO-BEE consortium, the Joint Controllers have entered into cooperation the subject of which is to conduct activities within the Project (hereinafter referred to as the "Cooperation");
B. the Cooperation requires that the Joint Controllers process personal data, whilst they jointly determine the purposes and means of processing of personal data;

C. the processing of personal data by the Joint Controllers requires that a transparent manner of determining their respective responsibilities be established as regards their compliance with the obligations under the 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 (hereinafter referred to as "General Data Protection Regulation" or "the GDPR"71) and other generally applicable laws as well as relations between the Joint Controllers and the data subjects;
D. on concluding this Arrangement, the Parties, seek to regulate the terms of processing of personal data in such a way that they meet the provisions of the GDPR, and
E. with regard to the data they process, the Joint Controllers act as controllers for the purposes of Article 24 et seq. of the GDPR referred to in D,

the Parties decided to enter into the following Arrangement:

§ 1.

Definitions

For the purposes of this Arrangement, the Parties agree that the following definitions and terms shall have the following meaning as defined in the GDPR:

1. **"Controller/Joint Controller"** means any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
2. **"Personal Data"** means any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject");
3. **"Third Country"** means any country that is not a member of the European Union or the European Economic Area or any international organisation;
4. **"Processor"** means any natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller;
5. **"Data Protection Law"** means the GDPR as well as other provisions of EU Member State's national law applicable to a relevant Party, passed in relation to personal data protection, including in particular the provisions of the given Controller's national law;
6. **"Processing**" means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
7. **"General Data Protection Regulation"**, **"GDPR"** means the 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; wherever this Arrangement refers to specific Articles of GDPR, it

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

shall also apply to the corresponding provisions in national legislation guaranteeing a similar level of safety;

8. **"Information System"** means a group of cooperating devices, programs, information processing procedures and program tools used for the purpose of data processing;
9. **"Cooperation"** means the cooperation between Controllers defined in Recital A;
10. **"Arrangement"** means this Arrangement on Joint Control of Personal Data;
11. **"Consortium Arrangement"** means the arrangement referred to in Recital A.

§ 2.

Subject-matter of the arrangement

1. This Arrangement regulates mutual relations between the Parties as regards the joint control of Personal Data, and in particular it determines in a transparent manner the Joint Controllers' responsibilities for compliance with the obligations under the GDPR; it also defines the representation of the Joint Controllers in contacts with the data subjects and their relations with those data subjects.
2. For the purpose of proper implementation of this Arrangement, the Joint Controllers shall:
    1) cooperate on performing the obligations of the Joint Controllers of Personal Data;
    2) process the Personal Data with which they have been entrusted with regard to the Cooperation pursuant to this Arrangement, GDPR, Consortium Agreement and other generally applicable laws and
    3) refrain from any legal or factual actions which might in any way undermine the security of Personal Data or threaten the other Joint Controller with civil, administrative or criminal liability.
3. Controllers' contact details shall be provided in Appendix 1 to the Arrangement.

§ 3.

Controllers' rights and obligations

1. The Joint Controllers declare that they have the means enabling them to process and protect Personal Data they are processing, including information systems meeting the requirements of the appropriate level of security, as stipulated by the GDPR. They will each fully adhere to the applicable Data Protection Law(s) with respect to obligations and responsibilities of controllers.
2. In particular, the Joint Controllers shall:
    1) exercise due diligence in processing Personal Data and process Personal Data pursuant to the Arrangement, the GDPR and other provisions of Data Protection Law(s), including the appropriate provisions of each Controller's national law;
    2) restrict access to Personal Data only to persons who need the access to Personal Data for the purposes of the Arrangement and Cooperation, provide those persons with relevant authorisations, offer relevant training on personal data protection and ensure confidentiality of Personal Data processed thereby, both during and after their employment or other cooperation with a Joint Controller;

3) assist the other Joint Controller, where possible, in meeting its (i) obligation to respond to requests from data subjects and (ii) obligations laid down in Articles 32 through 36 of the GDPR;

3. The Joint Controllers shall provide each other with the necessary assistance in carrying out the obligations referred to in section 2 point 3) above, in particular in the notification of a personal data breach, by:

    1) providing, at the request of a Controller, information concerning the processing of personal data immediately upon receipt of such request as soon as possible;

    2) notifying the other Joint Controllers of any breach as soon as possible but not later than 48 hours of its discovery. The notification should include all the information referred to in Article 33 (3) of the GDPR. If - and to the extent that - the information cannot be provided at the same time, they can be given successively without undue delay;

    3) providing to the other Joint Controllers all information necessary for the communication of a personal data breach to the data subject;

    4) informing the other Joint Controllers of inquiries, requests or demands from data subjects and other individuals, national or European Union public administrations, including relevant supervisory authorities and courts, as well as any controls or inspections by such authorities in connection with the joint controllership of Personal Data; information shall be provided promptly and in such a way as to enable the other Joint Controllers to comply with the obligations set out in sections 2 and 3, without undue delay but not later than 7 calendar days after receipt of an inquiry, request or demand or after the start of a control or inspection.

§ 4.

Data subjects' rights

1. The Joint Controllers shall inform, in any way they deem appropriate, the data subjects of the essences of this Arrangement and shall provide them the information referred to in Appendices 1 and 2 in accordance with Article 26 and Article 12 of the GDPR.
2. The information referred to in section 1 shall be primarily provided to the data subjects via email or by the Controller who collects the personal data.
3. Data subjects may contact any of the Joint Controllers about the rights granted to them by Articles 15 - 22 of the GDPR. The contacted Controller shall identify the responsible Controller and forward the request internally to this Controller. The originally contacted Controller shall carry out all necessary communication with the data subject.
4. The responsible Controller shall be determined as follows: If the data of the data subject is part of a set of data which can be attributed to a Controller, this Controller shall be responsible. In all other cases the Controller contacted by the data subject shall be the responsible Controller.
5. The Joint Controllers undertake to comply with the data subjects' rights and shall assist one another with the execution of data subjects' requests.

§ 5.

Transfers of Personal Data to third countries

Controller and/or its Processor(s) that transfer(s) personal data in the scope of the execution of the Arrangement to a Controller and/or Processor and/or other entity situated in the third country that does not present adequate safeguards under the GDPR shall ensure that such transfer is possible and that it complies with the GDPR (e.g. pursuant to Article 45 of the GDPR – on the basis of an adequacy decision Article 46.2.c) of GDPR – on the basis of standard data protection clauses adopted by the Commission in accordance with the examination procedure in Article 93.2 or pursuant to Article 49 of the GDPR. A copy of standard data protection clauses referred to in the preceding sentence shall be provided when so requested by a data subject.

§ 6.

Entrusting Processors with processing of Personal Data

1. The Controllers jointly consent to each of them entrusting Processors with processing of Personal Data subject to this Arrangement on terms and to the degree defined by this Arrangement and Article 28 of the GDPR.
2. Each Controller may entrust Processors with processing of Personal Data under this Arrangement only for the purposes of this Arrangement, Consortium Agreement and the Cooperation.
3. Processors can only carry out specific Personal Data processing activities on behalf of a Controller once the Controller has entered into a contract with such a Processor laying down the obligations of the latter related to Personal Data protection in a manner ensuring sufficient guarantees of technical and organisational measures for the processing to meet the requirements of the GDPR.
4. A Processor may carry out specific Personal Data processing activities on behalf of a Controller without entering into the contract referred to in section 3 as long as it is possible pursuant to another legal instrument under EU law or national law, which binds the Processor and the Controller.
5. This Paragraph shall apply in the case of any intended modifications regarding adding processors or replacing processors with other processors.
6. Where applicable, the Joint Controller shall provide detailed information on its Processors on request to the data subject.

§ 7.

Controllers' liability

The liability of the parties is governed by the legal regulations, in particular Article 82 of the GDPR with regard to the processing activities that they are in charge of as defined in regard of the Controller's role in the project and as stated in Appendix 1.

§ 8.

Collaboration of the Parties

1. The Parties shall cooperate in supervising the implementation of this Arrangement.
2. The Parties agree that at the time of the implementation of the Arrangement they shall cooperate closely, informing one another of any circumstances that have or may have effect on processing of Personal Data.
3. Each Party designates a contact point to coordinate the collaboration of the Parties in connection with the implementation of the Arrangement, disclosing their personal data in point 1 of the Appendix 2.
4. Amendments to Appendices 1 or 2 shall not require an amendment of the Arrangement, however all Parties shall have to be notified thereof either in writing or electronically by the Coordinator.

§ 9.

Term and termination of the Arrangement

1. The Arrangement will take effect as of the Effective Date.
2. This Arrangement can only be amended by the Parties following a consultation of all participating Parties, and provided that all participating Parties have agreed to the proposed amendment. If applicable law and regulations are amended, the Parties shall seek to amend this Arrangement accordingly.
3. The Arrangement shall be concluded for the period of implementation of the Cooperation and as long as and until, after the termination of the Cooperation, obligations still have to be fulfilled.

§ 10.

Final provisions

1. The Parties hereby agree that the Controllers shall process Personal Data pursuant to this Arrangement free of charge, and neither the conclusion of this Arrangement nor the processing of data pursuant thereto shall entitle any Controller to seek, on whatever legal basis,
    1) remuneration,
    2) reimbursement of any costs or expenses incurred for the purpose of due performance of the Arrangement,
    3) exemption from any obligations contracted to that end or advances on such costs or expenses,

even if at the time of entering into Cooperation or concluding this Arrangement, despite exercising due care, the Controller was unable to foresee the circumstances justifying such rises, costs, expenses or obligations.

2. Should any provision hereof become invalid or ineffective, the Parties shall adopt all measures possible to replace it with a valid and effective provision reflecting the goal and meaning of the invalid or ineffective provision to the extent of applicable law. Should any provision hereof be or become invalid or ineffective at any time, it shall not restrict the validity or effectiveness of the remaining provisions of the Arrangement.
3. In the event of any discrepancies between the provisions of the Arrangement and the terms of Cooperation agreed by the Parties, the provisions of this Arrangement shall prevail.
4. Any amendments hereto must be in writing on sanction of invalidity, subject to § 8 (4).
5. Any disputes arising under the Arrangement shall be resolved by amicably or by a common court with jurisdiction over the registered office of the Controller sued and pursuant to the laws applicable in its country.

This Arrangement shall be signed electronically by the Parties.

Signatures of the Parties:

Appendix 1: Controllers and processors in the SOCIO-BEE project

Controller	Role	Representative's name and contact details
CERTH	Project coordinator	Dr. Anastasios Drosou Email: drosou@iti.gr Tel.: +30 2311257701
AUTH	Technology provider	Mrs. Cornelia Vikelidou Email: data.protection@auth.gr Tel: +30 2310996200
BETTAIR	Technology provider	Email: dpo@bettaircities.com
NILU	Technology provider	Núria Castell Email: ncb@nilu.no
UDEUSTO	Pilot coordinator	Javier Garcia Zubia Email: zubia@deusto.es
UNIVPM	Technology provider	Dr. Rosalba Sacchettoni Email: rpd@univpm.it
HOPU	Technology provider	Email: iris@hopu.org
IBER	Technology provider	Francisco Sanz Email: ethics@ibercivis.es Tel: +34 976762995
ZKF	Technology provider	Raquel Povar Saz Email: rpovar@fundacionzcc.org
ZGZ	User partner (local community)	Email: dpd@zaragoza.es
MRSI	User partner (local community)	KaPa Data Consulting email: dpo@maroussi.gr Tel: +30 2106855245
ANCONA	User partner (local community)	Dr. De Luca Davide Email: privacy@pec.comuneancona.it Tel: 095 2935565

Appendix 2: Information to be provided to data subjects

INFORMATION

about processing of personal data within the SOCIO-BEE project

Pursuant to Article 13 of 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) (OJ. L 2016, No. 119, p. 1), we would like to inform you about the principles of processing of the personal data provided by you (information obligation):

1) The Joint Controllers of the Personal Data are as follows:

    1. ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (CERTH), established in CHARILAOU THERMI ROAD 6 KM, THERMI THESSALONIKI 57001, Greece, VAT number: EL099785242, *the Coordinator of the consortium*, and
    2. ARISTOTELIO PANEPISTIMIO THESSALONIKIS (AUTH), established in KEDEA BUILDING, TRITIS SEPTEMVRIOU, ARISTOTLE UNIV CAMPUS, THESSALONIKI 54636, Greece, and
    3. BETTAIR CITIES SL (BETTAIR), established in TRAVESSIA INDUSTRIAL 149 4C, HOSPITALET DE LLOBREGAT 08907, Spain, and
    4. NILU STIFTELSEN NORSK INSTITUTT FORLUFTFORSKNING (NILU), established in INSTITUTTVEIEN 18, KJELLER 2027, Norway, and
    5. UNIVERSIDAD DE LA IGLESIA DE DEUSTO ENTIDAD RELIGIOSA (UDEUSTO), established in AVENIDA DE LAS UNIVERSIDADES 24, BILBAO 48007, Spain, and
    6. UNIVERSITA POLITECNICA DELLE MARCHE (UNIVPM), established in PIAZZA ROMA 22, ANCONA 60121, Italy, and
    7. HOP UBIQUITOUS SL (HOPU), established in CALLE LUIS BUNUEL 6, CEUTI 30562, Spain, and
    8. FUNDACION IBERCIVIS (IBER), established in CALLE MARIANO ESQUILLOR SN CAMPUS RIO EBRO EDIFICIO I+D BLOQUE 2 PLANTA 2, ZARAGOZA 50018, Spain, and
    9. FUNDACION ZARAGOZA CIUDAD DE CONOCIMIENTO (ZKF), established in AVENIDA CIUDAD DE SORIA 8 EDIFICIO E2 PLANTA 6 DENTRO DEL ETOPIA, ZARAGOZA 50003, Spain, and
    10. AYUNTAMIENTO DE ZARAGOZA (ZGZ), established in PLAZA DEL PILAR 18, ZARAGOZA 50071, Spain, and
    11. MUNICIPALITY OF AMAROUSSION (MRSI), established in 9 VASILISSIS SOFIAS STR AND D. MOSCHA STR., AMAROUSSION 15124, Greece, and
    12. COMUNE DI ANCONA (ANCONA), established in PIAZZA XXIV MAGGIO 1, ANCONA 60124, Italy.

2) Data subjects should contact the project coordinator Dr. Anastasios Drosou at drosou@iti.gr in the following matters: personal data processing, exercise of rights related to personal data processing. In the event that any data subject reaches out to any other Joint Controller, they will forward the request to the project coordinator, who will address the request and deliver an answer back to the Joint Controller for reply to the data subject.

3) The Joint Controllers are consortium partners in the project SOCIO-BEE (Wearables and droneS fOr CIty Socio-Environmental Observations and Behavioral ChangE), funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement n° 101037648 – SOCIO-BEE. The Joint Controllers process personal data to perform pilot activities, including but not limited to technology development, testing and validation.

4) The Joint Controllers may process the collected personal data for periods required to perform Cooperation and obligations set forth in the consortium agreement concluded between the Joint Controllers and/or the grant agreement concluded between the Joint Controllers and the European Commission (hereinafter the Grant Agreement).

5) Data subjects – depending on the legal basis for processing – shall be entitled to the rights available to them pursuant to applicable laws, including as follows:
   a) to access to their personal data – which means that right to obtain from a Data Joint Controller a confirmation if their personal data are processed. If their data are processed, such data subjects are entitled to get access to their data and to obtain the following information: the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, the envisaged period for which the personal data will be stored or the criteria used to determine that period; the existence of the right to have the personal data corrected, erased or to restrict the processing of personal data and the right to object to the processing of the personal data (Article 15 of GDPR);
   b) to obtain a copy of the personal data being processed – the first copy is free of charge and for any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs (Article 15.3 of GDPR);
   c) to have incomplete personal data corrected, including by means of providing a supplementary statement (Article 16 of GDPR);
   d) to have their data deleted if a Data Joint Controller no longer has a legal basis to process the data or the data are no longer required to comply with the objectives of processing (Article 17 of GDPR);
   e) to have the processing restricted when: a data subject questions the accuracy of the personal data – for a period allowing the inspector to verify the accuracy of the data; the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; the Joint Controller no longer needs the personal data but they are required by the data subject for determining, pursuing and defending against any claims; the data subject has objected to processing pending verification as to whether the legitimate grounds of the Joint Controller override those of the data subject (Article 18 of the GDPR);
   f) to data portability – that is the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Joint Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller if the processing is based on consent of the data subject or on a contract concluded with the data subject and when the processing is carried out by automated means (Article 20 of GDPR);

g) the right to object to processing of their personal data for legitimate objectives of the Controller on grounds relating to their particular situation, including profiling. Then the Joint Controller will have to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. If, following such review, the interests of the data subject override the interests of the Controller, the Controller shall be obliged to discontinue the processing of the data in connection with objectives (Article 21 of GDPR);

h) the right to lodge a complaint with a supervisory authority if they consider that the processing of their personal data does not comply with of GDPR (Article 77 of GDPR).

6) The sharing of personal data during the project is required for the Joint Controllers to perform their duties, set out in the Grant Agreement n° 101037648 – SOCIO-BEE.

7) The scope of data processed during pilots shall be restricted to the required minimum which is as a rule set forth in the legal acts in force in the country of each Joint Controller. The collected data will not be used for any other purposes than those required for project activities, as resulting from the Consortium Agreement concluded between the Joint Controllers or from the Grant Agreement. The Joint Controllers may process the data for other legitimate purposes subject to the consent of the data subjects.

Annex VII – Research Ethics Protocol for Citizen Scientists

Research Ethics Protocol for SOCIO-BEE Citizen Scientists

The SOCIO-BEE project is a project funded by the European Union and runs from 2021 to 2024. SOCIO-BEE aims to encourage participants to take an active role in the action against climate change through citizen science using emerging technologies such as drones and wearables.

Having in mind that, as a SOCIO-BEE citizen scientist,

- *you become part of an inclusive and respectful community with a common goal towards opportunities for greater public engagement and scientific democratization;*
- *you act as contributor, collaborator, loudspeaker or as leader in activities organized by the SOCIO-BEE researchers;*
- *you have a meaningful role and you can contribute to a genuine science outcome. You will collectively help inform environmental policy by looking at better, (original, inventive) scientific methods to tackle air pollution in your area;*
- *you cooperate with professional researchers and will be invited to participate in defining the research question, designing the method, gathering and analyzing data, and communicating the results taking the scientific replicability/reproducible principle in mind;*
- *you will receive guidance and feedback from the SOCIO-BEE researchers about how the data you collect is being used and how your contribution impacts the world around you;*
- *you will contribute in identifying possible limitations and biases of the research project you participate in and you reckon how your personal, social and cultural backgrounds influence thinking and conclusions obtained,*
- you agree with the goals and principles of the SOCIO-BEE community
    - Why is this important?
        - To have a common vision, which will make our shared ambition feasible
- you agree to take part in the SOCIO-BEE co-creation space to suggest new ideas, recommend improvements and participate in decision making
    - Why is this important?
        - To make your voice heard
        - To allow for cooperation and dialogue
- you agree to follow the instructions by the SOCIO-BEE researchers during the SOCIO-BEE activities. Sometimes, we will invite you to participate in trainings and workshops to better understand the project work and your role in it
    - Why is this important?
        - To stay safe
        - To improve and ensure the quality of your collected data for further research
        - To respect the rights and freedoms of fellow participants
- you agree to use the tools provided to you only for purposes related to the SOCIO-BEE activities. We will be there for you if you have questions or concerns at any stage of the project and you are encouraged to ask any time
    - Why is this important?
        - To stay safe
        - To improve and ensure the quality of your collected data for further research
        - To respect the rights and freedoms of fellow participants and citizens

- your contribution will be acknowledged as SOCIO-BEE citizen scientist in relevant publications and activities
    - Why is this important?
        - As a citizen scientist, you contribute equally to the scientific outcome
- if you feel discomfort or simply you do not wish to participate any more, you can withdraw from the project without any detrimental consequence for you at any point. You will have someone looking after you with whom - if you wish - you can discuss the reasons for withdrawal and address any concern that the methodology or participation may have caused to you in order to learn from it and provide a solution in next iterations.
    - Why is this important?
        - You participate in the SOCIO-BEE activities voluntarily
        - To keep a safe space where everyone feels that can equally participate
- if you do not follow the instructions of the SOCIO-BEE researchers or you misuse the tools provided to you, the SOCIO-BEE researchers kindly reserve the right to remove you from your role as citizen scientist, after explaining the reasons for this decision
    - Why is this important?
        - To allow for respectful cooperation between all sides
        - To ensure everyone's safety
- if at any point you feel excluded by either the language, behaviours or actions by any of the researchers or other participants, we will make sure there is an easy and comfortable way for you to inform us
    - Why is this important?
        - To help us improve our inclusion policies
        - To ensure you and everyone feels safe and happy to contribute

Annex VIII – Final for Information sheets and consent forms for research participants and processing of personal data

What is SOCIO-BEE?

SOCIO-BEE (Wearables and droneS fOr CIty Socio-Environmental Observations and BEhavioral ChangE) is a Horizon 2020 project (Grant agreement ID: 101037648), that started in October 2021 and will run until September 2024. Citizens and their communities, particularly those that are vulnerable to the impacts of climate change, can play an important role in achieving climate neutrality. Scientists are developing social innovation tools to empower communities to adopt pro-environment actions and sustainable behaviours aligned with environmental policy. Inspired by the bee metaphor (worker and drone bees as main 'citizen science actors'), EU-funded SOCIO-BEE will study the facilitation of structures to increase citizen engagement and awareness of climate change through experimentation and monitoring of the environment. The project aims to develop low-cost technological innovations and instruments that will tangibly contribute to the overall pro-climate campaign, with primary focus on improving air-quality in urban areas.

The project coordinator is CERTH (ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS). The project consists of 18 partners from 7 countries.

You can find more information about the project, by visiting [ADD website and project social media].

Conditions for the participation in the research

- Inform the participants that the study is entirely voluntary and ensure that there is no pressure or coercion for them to take part.
- Inform the participants that they can refuse to participate or withdraw from the study at any time without consequences.

Purposes of the research

- Clearly explain the purposes of the research

Contact for the specific research activity

- Include information about the organisation/person in charge of the study as well as the contact details for the organisation/person in charge for the provision of information relation to the research and the contact of the organisation/person in charge for assisting in the event of a research-related injury.

How long am I expected to participate in this research?

- State the expected duration of the subject's participation and whether the study is one-off or requires repeated participation and/or a follow-up, how often and where.

What is the research methodology?

- Describe the procedures and the methodology to be followed. How will you process the data you will collect?

What I am expected to do during my participation?

- Describe the technology/software/platform/tool to be tested or activity to participate and what is expected by the participant.

Are there any risks for me?

- Inform about foreseeable risks, or any discomfort or disadvantages that the participation to the study may entail for the research participant.

What are the benefits for me?

- Inform about benefits to the subject or to others from the study.

Will I receive payment?

XXX

Our incidental findings policy

XXX

What about the results of the research?

- Inform about what will happen to the results of the research (where they will be published) and how/whether the research participant can be informed about them, if they wish.

Covid-19 statement

SOCIO-BEE researchers further commit to observe any particular frameworks developed at EU and national level concerning necessary safeguards for carrying out research with human participants during the Covid-19 pandemic and will ensure that both the safety of the researchers and the participants is respected in line with the specific requirements and measures.

Consent form for the participation in the SOCIO-BEE research project

I, undersigned [name] [date and place of birth] [natural person; legal entity] [contact details] [if representing a minor: her/his/xx name, date of birth, etc.], I declare that:

- ☐ I have been informed that the SOCIO-BEE project is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. [number]. The co-ordinator of the project is [name]. The coordinator of the project may be contacted at [contact details]. The coordinator of this study may be contacted with regard to any question about my participation at [contact details]. I have been informed that in case of injury, I can contact [name] at [contact details].
- ☐ I have read and understood the Research Ethics Protocol for SOCIO-BEE Citizen Scientists and I abide by its principles.
- ☐ I have been informed about the purposes of the project and I have fully understood what my
- ☐ participation to the study entails from my side [tasks].
- ☐ I had enough time to think and I have been able to ask all the questions that have come to mind and I have received a clear answer to those questions.
- ☐ I have fully understood that my participation is entirely voluntary and that I can withdraw at any time without any detriment consequences.
- ☐ I understand [I will / I will not] be paid for my participation.
- ☐ I understand the risks that my participation to this research may carry.
- ☐ I understand the benefits that my participation to this research entails.
- ☐ I understand that the laws of [country] shall apply.

I hereby give my consent to take part in the research carried out by [the SOCIO-BEE Consortium/specific partner]

Done at [place] on [date]
Full name
Signature (by the participant or the legal guardian)

Done in two copies (one for the research participant and one to be kept in the SOCIO-BEE records).

Statement of the researcher

I hereby declare that the participant has been informed to the best of my knowledge about the research activity. The participant received the present information sheet and consent form and explanations. The participant received an original copy and I have saved the second original copy in the SOCIO-BEE records.

I, the undersigned [surname, first name], researcher, hereby declare that I have provided the required information about this study orally, as well as a copy of the information sheet and the consent form to the participant.

I confirm that no pressure has been exerted on the participant to have their consent to participate in the study. I also declare that I have answered any questions that were addressed to me to the best of my knowledge.

I confirm that I work in accordance with the ethical principles within my specific research discipline.

Done at [place] on [date]
Full name
Signature by the researcher

Ensure that the whole document is stapled/kept together.

Information Sheet for personal data protection related matters in SOCIO-BEE

The Information Sheet for data protection related matters should include de minimis the following bullets

What is SOCIO-BEE?

SOCIO-BEE (Wearables and droneS fOr CIty Socio-Environmental Observations and BEhavioral ChangE) is a Horizon 2020 project (Grant agreement ID: 101037648), that started in October 2021 and will run until September 2024. Citizens and their communities, particularly those that are vulnerable to the impacts of climate change, can play an important role in achieving climate neutrality. Scientists are developing social innovation tools to empower communities to adopt pro-environment actions and sustainable behaviours aligned with environmental policy. Inspired by the bee metaphor (worker and drone bees as main 'citizen science actors'), EU-funded SOCIO-BEE will study the facilitation of structures to increase citizen engagement and awareness of climate change through experimentation and monitoring of the environment. The project aims to develop low-cost technological innovations and instruments that will tangibly contribute to the overall pro-climate campaign, with primary focus on improving air-quality in urban areas.

The project coordinator is CERTH (ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS). The project consists of 18 partners from 7 countries.

You can find more information about the project, by visiting [ADD website and project social media].

Who is the Data Controller?

- Provide the information of the data controller and of the Data Protection Officer or the person in charge of providing assistance in relation to data protection matters in your organisation.

What personal data do we collect/process?

- Explain which personal data will be collected and processed and how these data will be collected and processed (your sources and tools).

For which purposes do we collect/process those personal data?

- Describe the purposes of the data processing.

What is the legal basis that allows us to process your data?

- Explain **the legal basis for <u>each data processing operation</u>** (for research: consent or public interest (if public authority) / for events: legitimate interest may apply as well, eg video recordings)

How long does the storage of your data last?

- Explain for how long the data controller will store the personal data and what will happen with the data at the end of the research period, in particular, if the data are retained or sent to a third party for further research.

The personal data matrix (not mandatory, but highly recommended)[72]

You can provide a summary of the above information in a table.

Personal data	Source	How and why? (Purpose)	Legal basis	Storage	Any other information
Full name	*You provide it to us*	To store your consent form; to contact you with a follow up of the research	Consent	Duration of the project + 6 months	/

What are my rights?

- Explain the data subject's rights, including the right of a data subject to lodge a complaint with the respective supervisory authority.

How do you keep my personal data secure?

- Describe the procedures adopted for ensuring data security (integrity and confidentiality) in response to specific risks you may encounter.

Will a third party outside the SOCIO-BEE consortium have access to my data?

- Explain whether the processing will occur exclusively by the data controller, or a data processor will be engaged and provide the information of the data processor.

Will you transfer my personal data to countries outside the European Union?

- State whether personal data will be transferred outside the European Union, to a third country and under which conditions.

Contact information of the project coordinator, the data controller and the DPO

- Provide again the info.

Consent form[73]

I, undersigned [name] [date and place of birth] [natural person; legal entity] [contact details] [if representing a minor: her/his/xx name, date of birth, etc.], I declare that:

- ☐ I understand that my personal data will be made available only to the SOCIO BEE Consortium and the European Commission, if requested.
- ☐ I was informed about the nature, the purposes and the context of the processing.
- ☐ I was informed about my rights as a data subject, including my right to lodge a complaint with
- ☐ the relevant supervisory authority.

[72] All the matrices will also be included in the D6.2 and D6.3. The information in the table is an example.
[73] If your legal basis is consent

- ☐ I was given the contact details of the project coordinator, the data controller and the data protection officer and I understand that I can contact them for any relevant questions in relation to the processing of my personal data.
- ☐ I understand that no further use of my personal information in the course of the project is foreseen.[74]
- ☐ I understand that I am free to withdraw my consent for the processing of my personal data at any time without any negative consequences.
- ☐ I was informed about the risks arising from the processing and about the safeguards put in place to mitigate them.
- ☐ I require my participation remains anonymous and that I will not be identified in any research results.[75]
- ☐ I understand that the laws of [country] shall apply.
- ☐ I hereby give my consent for my personal data to be processed by [the SOCIO BEE Consortium /Organisation] for [the purposes of the respective research].

Done at [place] on [date]
Full name
Signature (by participant or legal guardian)

- ☐ I hereby give my explicit consent for [specify which special categories of data] to be processed by [the SOCIO BEE Consortium/organisation] for [the purposes of the respective research][76]

Done at [place] on [date]
Full name
Signature (by participant or legal guardian)

Done in two copies (one for the research participant and one to be kept in the SOCIO BEE records)

[74] If that's not the case, you have to indicate it and acquire the explicit consent.
[75] You can also provide a clause, to allow the data subject to be identified, if that's the purpose of the research, e.g. if you want to use a quote.
[76] If applicable

Annex X – Privacy notice for ACADE-ME app

PRIVACY NOTICE

Summary

Joint Data Controllers	CERTH, AUTH, BETTERAIR, NILU, UDEUSTO, UNIVPM, HOPU, IBER, ZKF, ZGZ, MRSI, ANCONA
Purposes	(i) Enrolment as citizen scientist; (ii) participation on the Project as citizen scientist and use of the App, (iii) improvement of the App
Legal basis	Consent, for the first purpose, and legitimate interest, for the second and third purpose
Data Processors and other recipients	All information will be processed within the joint controllers
Data Subject's Rights	withdrawn consent, access right, rectification right, erasure right, restriction right, data portability, objection right
Additional Information	Not applicable

Last updated May 16, 2023

This privacy notice ('**Notice**') applies to the use of the ACADE-ME app ('**App'**), which is intended to be used within the context of the SOCIO-BEE Project, funded by the European Commission under grant no. 959201 ('**Project**'). The App is provided by ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS ('**Coordinator**'), acting as representative of the joint data controllers ('**we**', '**us**', or '**our**'), listed below:

1. ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (CERTH), established in CHARILAOU THERMI ROAD 6 KM, THERMI THESSALONIKI 57001, Greece, VAT number: EL099785242, the Coordinator of the consortium, and
2. ARISTOTELIO PANEPISTIMIO THESSALONIKIS (AUTH), established in KEDEA BUILDING, TRITIS SEPTEMVRIOU, ARISTOTLE UNIV CAMPUS, THESSALONIKI 54636, Greece, and
3. BETTAIR CITIES SL (BETTAIR), established in TRAVESSIA INDUSTRIAL 149 4C, HOSPITALET DE LLOBREGAT 08907, Spain, and
4. NILU STIFTELSEN NORSK INSTITUTT FORLUFTFORSKNING (NILU), established in INSTITUTTVEIEN 18, KJELLER 2027, Norway, and

5. UNIVERSIDAD DE LA IGLESIA DE DEUSTO ENTIDAD RELIGIOSA (UDEUSTO), established in AVENIDA DE LAS UNIVERSIDADES 24, BILBAO 48007, Spain, and
6. UNIVERSITA POLITECNICA DELLE MARCHE (UNIVPM), established in PIAZZA ROMA 22, ANCONA 60121, Italy, and
7. HOP UBIQUITOUS SL (HOPU), established in CALLE LUIS BUNUEL 6, CEUTI 30562, Spain, and
8. FUNDACION IBERCIVIS (IBER), established in CALLE MARIANO ESQUILLOR SN CAMPUS RIO EBRO EDIFICIO I+D BLOQUE 2 PLANTA 2, ZARAGOZA 50018, Spain, and
9. FUNDACION ZARAGOZA CIUDAD DE CONOCIMIENTO (ZKF), established in AVENIDA CIUDAD DE SORIA 8 EDIFICIO E2 PLANTA 6 DENTRO DEL ETOPIA, ZARAGOZA 50003, Spain, and
10. AYUNTAMIENTO DE ZARAGOZA (ZGZ), established in PLAZA DEL PILAR 18, ZARAGOZA 50071, Spain, and
11. MUNICIPALITY OF AMAROUSSION (MRSI), established in 9 VASILISSIS SOFIAS STR AND D. MOSCHA STR., AMAROUSSION 15124, Greece, and
12. COMUNE DI ANCONA (ANCONA), established in PIAZZA XXIV MAGGIO 1, ANCONA 60124, Italy.

The Notice describes how and why we might collect, store, use, and/or share ('**process**') your information when you use the App for the intended services ('**Services**').

Questions or concerns**?** Reading this privacy notice will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact the project coordinator at drosou@iti.gr.

0. Introduction

The data processing on the App is pursuant to the provision of the EU General Data Protection Regulation (GDPR), and in accordance with the country-specific data protection regime applicable to the Coordinator, headquartered in Greece (EU Member State). For further information, please check Section 2 of the present data protection policy.

Personal data, as defined by Article 4(1) General Data Protection Regulation (GDPR) include any information relating to an identified or identifiable living natural person. Personal data can be your first name, last name, e-mail address, email format and IP address.

1. General information: What is the Project?

SOCIO-BEE is a research project that has received funding from European Commission under grant no. 959201. The project started on October 1, 2021 and ends on September 30, 2024.
The present App is part of the SOCIO-BEE portal where users can engage with the citizens science aspect of the Project.

2. Contact information of the data controller and of the Data Protection Officer

The Data Protection Officer at the Coordinator may be reached at spapastergiou@certh.gr.
In case you have any questions about the processing of your data when using the App or your rights as data subject, you can also submit your query via our contact form, with the indication "Data Protection Inquiry".

3. Data Handling, Legal basis and Purpose of the processing

Data Matrix template

Personal data	Processing and purpose of the processing	Legal basis of the processing	Retention location and period
Identification-Related Personal Data Provided by You: • Names; • Email addresses; • Usernames; • Passwords; • Contact or authentication data.	Interactions with us and the Services, the choices you make, and the products and features you use.	Consent - Art. 6.1.(a) GDPR	CERTH based SOCIO-BEE dedicated server during Project duration.
Application Data: • Audiovisual data. • Geolocation Information. • Mobile Device Access. • Mobile Device Data. • Push Notifications.	We may request access or permission to track location-based information from your mobile device, either continuously or while you are using our mobile application(s), to provide certain location-based services. Moreover, we	Legitimate interest – Art. 6.1.(f)	CERTH based SOCIO-BEE dedicated server during Project duration.

Personal data	Processing and purpose of the processing	Legal basis of the processing	Retention location and period
• Activity Logs. • Data about your volunteering activities. • The feedback you give through the app, in order to help us improve the app.	will collect audiovisual information through your smartphone sensors. Send you push notifications regarding your account or certain features of the application(s). Troubleshoot the problems of the application and create more informed suggestions. Maintain the security and operation of our application(s), for troubleshooting, and for our internal analytics and reporting purposes. Summarise the volunteering outcomes and also be able to make better suggestions to you. Improve the app.		
Pollution Data: • Exposure to air pollution.	As part of the citizens' science experiment to be conducted under the Project, we will collect information about your exposure to air pollution through the corresponding devices.	Legitimate interest – Art. 6.1.(f)	CERTH based SOCIO-BEE dedicated server during Project duration.

4. When and with whom do we share your personal information?

All the information that we collect about you during the course of the research will be kept strictly confidential. You will not be able to be identified in any publications. The results of this investigation may be published in reports, scientific journals or conferences and used in further studies, but it will not be possible to identify the source of the information. Nothing of the provided data will be handed out to third parties. The authorization for the use and access to your information is valid until the end of the project, unless you decide to cancel it before. Your decision whether or not to give your authorization for the use and diffusion of the information provided by you is completely voluntary. Nevertheless, we may be required by the **European Commission** as our funder to share data with them in accordance with the European Commission's internal rules, or other entities nominated by the European Commission (e.g., expert reviewers).

5. Your rights as a data subject

As a data subject, you have the following rights:

- pursuant to Article 7(3) GDPR, to **withdraw your consent at any time and without any consequences for you.** This means that in future we may no longer continue to process the data as based on this consent;
- pursuant to Article 15 GDPR, to **obtain information** about whether your personal data are processed by us and where that is the case, access to those personal data. In particular, you may obtain information about the purpose of processing, the category of the personal data, the categories of recipients, to whom your data has been or is disclosed to, the storage period planned, the existence of a right to request from the controller rectification, erasure, restriction of processing or objection, the existence of a right to lodge a complaint and the source of your data if it has not been collected by us. Pursuant to Article 12, we must provide any communication relating to the processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- pursuant to Article 16 GDPR, to **obtain the rectification of inaccurate personal data** without undue delay or the completion of your personal data stored with us;
- pursuant to Article 17 GDPR, to **obtain the erasure of your personal data** stored with us unless processing is necessary to exercise the right to freedom of expression and information, for compliance with a legal obligation, for reasons of public interest, or to establish, exercise or defend legal claims;
- pursuant to Article 18 GDPR, to **obtain the restriction of the processing of your personal data**;
- pursuant to Article 20 GDPR, to **receive your personal data, in a structured, commonly used and machine-readable format** or to obtain the transmission to another data controller (right to data portability);
- pursuant to Article 21 GDPR, to **object**, on grounds relating from your particular situation, at any time to processing of your personal data, which is based on data processing for the purposes of legitimate interests. If you file an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or unless processing serves the establishment, exercise or defence of legal claims.

If you wish to exercise your rights or you wish to receive more information, please go to Section 2 - Contact information, where you can find the most updated contact information.

Pursuant to Article 77 GDPR, you also have the right to **lodge a complaint** with a national supervisory authority. You can contact the supervisory authority of your habitual residence or workplace or of our Coordinator. In the latter case, you can file a complaint with the Hellenic Data Protection Authority.

6. Data security

Moreover, we use suitable technical and organisational measures, which are being continuously enhanced, to protect your data against accidental or intentional manipulation, partial or complete loss, destruction or against unauthorised access by third parties not involved directly in the Project.

7. Amendments to this Data Protection Policy

This data protection policy is effective as of May 16, 2023. The policy was reviewed and amended in May 16, 2023.
We keep our Data Protection Policy under regular review to make sure it is up to date and precise. Thus, it may become necessary to change it due to the potential addition of new features to the App or due to further legal requirements.

Annex XI – End User License Agreement for ACADE-ME app

EULA Preview

END USER LICENCE AGREEMENT

Last updated May 16, 2023

ACADE-ME SOCIO-BEE app ('**Licensed Application**') is licensed to you ('**End User**') by the relevant members of the SOCIO-BEE Project, funded by the European Commission under grant no. 959201 ('**Licensor**'), represented in this act by ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS, for use only under the terms of this agreement ('**License Agreement**').

The SOCIO-BEE project aims to design, deploy and validate a next-generation CS platform for citizens' wearable-based modules for air quality observation, supported by local decision-makers and action groups ('**Project**').

SOCIO-BEE aims to realize sustainable, scalable, and replicable/spreadable experiments, which are co-created. SOCIO-BEE will develop and implement a co-creation module for facilitating citizen science. Users will be able to select among several **customizable campaigning blueprints** each of which will entail such tools for delivering engagement programmes and campaigns that genuinely enable communities to influence decision making for reducing pollution levels in cities and creating trust between stakeholders.

By downloading the Licensed Application from the Project's authorized channels, which might include in the future Google's software distribution platform ('**Play Store'** and together with any future software distribution platform used for the Licensed Application, '**Services**'), and any update thereto (as permitted by this License Agreement), the End User indicates its agreement to be bound by all of the terms and conditions of this License Agreement.

The parties of this License Agreement acknowledge that the Services are not a Party to this License Agreement and are not bound by any provisions or obligations with regard to the Licensed Application, such as warranty, liability, maintenance and support thereof. SOCIO-BEE, not the Services, is solely responsible for the Licensed Application and the content thereof.

This Licence Agreement may not provide for usage rules for the Licensed Application that are in conflict with the latest Google Play Terms of Service ('**Usage Rules**'). SOCIO-BEE acknowledges that it had the opportunity to review the Usage Rules and this Licence Agreement is not conflicting with them.

SOCIO-BEE app when downloaded through the Services, is licensed to the End User for use only under the terms of this Licence Agreement. The Licensor reserves all rights not expressly granted to You. SOCIO-BEE app is to be used on devices that operate with Google's operating system (**'Android**').

1. LICENSED APPLICATION

SOCIO-BEE app is a piece of software created to support the co-creation process in SOCIO-BEE project — and customized for Android mobile devices ('**Devices**'). The Licensed Application will interact with project-approved wearables and its cloud services, particularly its web interface. In particular, the Licensed Application will be used for:

- participating in micro volunteering tasks based on the End User's location;
- retrieving data regarding citizens' exposure to pollutants;
- producing individuals' exposure to air pollution analytics through data combination;
- tracking individuals' routes for the generation of expected exposure to pollution in those routes; and
- generating analytics for the expected exposition to pollution of the mean citizen, after aggregating the results of the individual users.

2. SCOPE OF LICENCE

2.1 Licensor grants a non-exclusive, non-transferable, revocable license to use the Licensed Application for the End User's personal, noncommercial use within the context of the Project ('**License**').

2.2 The License will automatically end upon the Project's termination, currently scheduled for September 30, 2024.

2.3 Licensor reserves the right to modify the terms and conditions of the License. These changes will be notified to the End User upon first access to the Licensed Application after any modification is made by the Licensor.

2.4 Nothing in this License should be interpreted to restrict third-party terms. When using the Licensed Application, the End User must ensure its compliance with applicable third-party terms and conditions.

3. TECHNICAL REQUIREMENTS AND SUPPORT

3.1 The Licensed Application requirements will be communicated upon installation of the App.

3.2 Licensor attempts to keep the Licensed Application updated so that it complies with modified/new versions of the firmware and new hardware. The End User is not granted rights to claim such an update.

3.3 The End User acknowledges that it is its responsibility to confirm and determine that its device is capable of running the Licensed Application.

3.4 Licensor reserves the right to modify the technical specifications as it sees appropriate at any time.

3.5 The Licensor is solely responsible for providing any maintenance and support services for this Licensed Application as long as the License has not been terminated. You can reach the Licensor at the email address listed in the Play Store Overview for this Licensed Application.

4.2 The Licensor and the End-User acknowledge that the Services have no obligation whatsoever to furnish any maintenance and support services with respect to the Licensed Application.

4. USER-GENERATED CONTRIBUTIONS

4.1 The Licensed Application will ask End User to provide a wide range of contributions within the context of the Project, such as: data generated from your smartphone sensors, including audio, visual, and global positioning system (GPS) data; information on the End User's behaviour; and exposure to air pollution (collectively, 'Contributions').

4.2 With respect to the Contributions, the End User represent and warrant that:

1. The creation, distribution, transmission, public display, or performance, and the accessing, downloading, or copying of the Contributions do not and will not infringe the proprietary rights, including but not limited to the copyright, patent, trademark, trade secret, or moral rights of any third party.
2. It is the creator and owner of or have the necessary licenses, rights, consents, releases, and permissions to use and to authorize us, the Licensed Application, and other users of the Licensed Application to use the Contributions in any manner contemplated by the Licensed Application and this License.
3. You have the written consent, release, and/or permission of each and every identifiable individual person in the Contributions to use the name or likeness or each and every such identifiable individual person to enable inclusion and use of the Contributions in any manner contemplated by the Licensed Application and this License.
4. The Contributions are not false, inaccurate, or misleading.
5. The Contributions are not unsolicited or unauthorized advertising, promotional materials, pyramid schemes, chain letters, spam, mass mailings, or other forms of solicitation.
6. The Contributions are not obscene, lewd, lascivious, filthy, violent, harassing, libelous, slanderous, or otherwise objectionable (as determined by us).
7. The Contributions do not ridicule, mock, disparage, intimidate, or abuse anyone.
8. The Contributions are not used to harass or threaten (in the legal sense of those terms) any other person and to promote violence against a specific person or class of people.
9. The Contributions do not violate any applicable law, regulation, or rule.
10. The Contributions do not violate the privacy or publicity rights of any third party.
11. The Contributions do not violate any applicable law concerning child pornography, or otherwise intended to protect the health or well-being of minors.
12. The Contributions do not include any offensive comments that are connected to race, national origin, gender, sexual preference, or physical handicap.

13. The Contributions do not otherwise violate, or link to material that violates, any provision of this License, or any applicable law or regulation.

4.3 Any use of the Licensed Application in violation of the foregoing violates this License and may result in, among other things, termination or suspension of your rights to use the Licensed Application.

4.4 By making the Contributions accessible for the Licensed Application, the End User automatically grant, and you represent and warrant that you have the right to grant, to us an unrestricted, unlimited, irrevocable, non-exclusive, transferable, royalty-free, fully-paid, worldwide right, and license to host, use copy, reproduce, disclose, sell, resell, publish, broad cast, retitle, archive, store, cache, publicly display, reformat, translate, transmit, excerpt (in whole or in part), and distribute such Contributions (including, without limitation, your image and voice) for any purpose, commercial advertising, or otherwise, and to prepare derivative works of, or incorporate in other works, such as Contributions, and grant and authorize sublicenses of the foregoing. The use and distribution may occur in any media formats and through any media channels.

4.5 The Licensor is not liable for any statements or representations in the Contributions provided by the End User in any area in the Licensed Application. The End User is solely responsible for them expressly agree to exonerate the Licensor from any and all responsibility and to refrain from any legal action against it regarding the Contributions.

5. LIABILITY

To the maximum extent permitted by applicable law, in addition to the above warranty disclaimers, in no event will the Licensor be liable for any consequential, exemplary, special or incidental damages, including any damages for lost data or lost profits, arising from or relating to the products or products software, whether in contract or tort or otherwise arising from (1) any action you may take in reliance on the information, (2) the use or inability to use our services, (3) third party services outside our reasonable control and for the avoidance of doubt and whether or not the relevant loss arises by reason of our negligence. Nothing in this License Agreement shall exclude our liability for personal injury or death or for fraudulent misrepresentation.

6. WARRANTY

6.1 Licensor warrants that the Licensed Application is free of spyware, Trojan horses, viruses, or any other malware at the time of the End User's download. Licensor warrants that the Licensed Application works as described in the user documentation.

6.2 No warranty is provided for the Licensed Application that is not executable on the device, that has been unauthorized modified, handled inappropriately or culpably, combined or installed with inappropriate hardware or software, used with inappropriate accessories, regardless if by the End User or by third parties, or if there are any other reasons outside of the Licensor's sphere of influence that affect the executability of the Licensed Application.

6.3 The End User is required to inspect the Licensed Application immediately after installing it and notify the Licensor about issues discovered without delay by email provided in contact information section below. The defect report will be taken into consideration and further investigated if it has been emailed within a period of thirty (30) days after discovery.

6.4 If the Licensed Application is confirmed to be defective, the Licensor reserves a choice to remedy the situation either by means of solving the defect or substitute delivery.

7. PRODUCT CLAIMS

The Licensor and the End-User acknowledge that the Licensor, and not the Services, is responsible for addressing any claims of the End-User or any third party relating to the Licensed Application or the End-User's possession and/or use of that Licensed Application, including, but not limited to:

(i) product liability claims;

(ii) any claim that the Licensed Application fails to conform to any applicable legal or regulatory requirement; and

(iii) claims arising under consumer protection, privacy, or similar legislation, including in connection with the Licensed Application's use of the HealthKit and HomeKit.

8. CONTACT INFORMATION

For general inquiries, complaints, questions or claims concerning the Licensed Application, please contact the Project supervisor dr. Anastasios Drosou at drosou@iti.gr.

9. TERMINATION

9.1 The License Agreement is valid until the term set in clause 2.2, or until terminated by the Licensor or the End User.

9. 2 The End User's rights under this License Agreement will terminate automatically and without notice from the Licensor if it fails to adhere to any term(s) of this license.

9.3 Upon the License Agreement termination, the End User shall stop all use of the Licensed Application, and destroy all copies, full or partial, of the Licensed Application.

10. THIRD-PARTY TERMS OF AGREEMENTS AND BENEFICIARY

The Licensor represents and warrants that it will comply with applicable third-party terms of agreement when using Licensed Application.

In Accordance with Section 9 of the 'Instructions for Minimum Terms of Developer's End-User License Agreement', both Apple and Google and their subsidiaries shall be third-party beneficiaries of this End User License Agreement and — upon Your acceptance of the terms and conditions of this License Agreement, both Apple and Google will have the right (and will be deemed to have accepted the right) to enforce this End User License Agreement against You as a third-party beneficiary thereof.

11. INTELLECTUAL PROPERTY RIGHTS

The Licensor and the End-User acknowledge that, in the event of any third-party claim that the Licensed Application or the End-User's possession and use of that Licensed Application infringes on the third party's intellectual property rights, the Licensor, and not the Services, will be solely responsible for the investigation, defence, settlement, and discharge or any such intellectual property infringement claims.

12. APPLICABLE LAW

This Licensing Agreement shall be governed by and construed and enforced in accordance with the laws of the Hellenic Republic (‘**Greece**’), and shall be interpreted in all respects as a Greek agreement. Any claim or action arising from or related to this Licensing Agreement shall be governed by and construed and enforced in accordance with the laws of Greece. For the avoidance of doubt, and without limiting the generality of the foregoing, this provision expressly applies to any tort claim against the Licensor. The End User unconditionally attorn to the exclusive jurisdiction of the courts of Greece and all courts competent to hear appeals therefrom. The doctrine of *forum non convenient* shall not apply in the selection of forum under this Licensing Agreement.

13. MISCELLANEOUS

13.1 If any of the terms of this agreement should be or become invalid, the validity of the remaining provisions shall not be affected. Invalid terms will be replaced by valid ones formulated in a way that will achieve the primary purpose.

13.2 Collateral agreements, changes and amendments are only valid if laid down in writing. The preceding clause can only be waived in writing.