CommuniCity

Innovative Solutions Responding

to the Needs of Cities & Communities

D7.1 Data Management Plan v.1.0

Funded by
the European Union

D7.1 Data Management Plan v1.0

Project acronym: **CommuniCity**

Project full title: **Innovative Solutions Responding to the Needs of Cities & Communities - CommuniCity**

Grant agreement no.: 101070325

Delivery Date:	15/11/2023
Lead Partner:	OASC
Editors:	Hugo Kerschot, Josephine Di Pino (OASC)
Reviewers:	Martin Brynskov (OASC), Sennay Ghebreab (UA)
Dissemination Level:	PU (public)
Version:	V1.0

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HaDEA). Neither the European Union nor the granting authority can be held responsible for them.

REVISION HISTORY

Date and version number	Contributor	Comments
v0.1, 07/03/2023	Josephine Di Pino	initial draft
v0.2, 07/12/2023	Hugo Kerschot	Update
v0.3, 11/12/2023	Martin Brynskov, Sennay Ghebreab	Review
v0.4, 13/12/2023	Hugo Kerschot	processing reviewers remarks
v0.5, 14/12/2023	External Ethics board	Review
v0.6, 15/12/2023	Hugo Kerschot	processing Ethics board members remarks
v1.0, 15/10/2023	Hugo Kerschot	Final version

Table of contents

Executive Summary

The CommuniCity project is a Coordination and Support Action with the specific goal to support 100 tech pilots in Europe in urban and peri-urban areas to empower marginalised communities.

In this perspective data management for this project has also two aspects. On one hand the data management of the project with its deliverables and communication/dissemination content and the data management of the individual selected pilots… this last one is a very specific challenge for the project.

This first version of the Data Management Plan will focus on the project management aspect of the project as such, based on Open Data Access Policy and FAIR data principles as well as Data security and Ethics and some first learnings and reflections on the data management aspects of the first two experimental calls.

Since the project has as main objective to develop a methodology and infrastructure for piloting digital solutions for vulnerable and marginalised communities, these data management aspects at the pilot level and how to handle these in the context of large-scale calls will be the focus of the second Data Management Plan at the end of the CommuniCity project.

Introduction

The CommuniCity Data Management Plan (DMP) defines how data generated or collected within this project will be treated, archived, disseminated and maintained by the project partners and how the data will be shared with the wider community, e.g., via the CommuniCity website.

The purpose of this document is to present how the data within the CommuniCity project is managed in a **FAIR** (Findable, Accessible, Interoperable and Reusable) manner. It follows the "Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020" and "Guidelines on FAIR Data Management in Horizon 2020" within the H2020 Programme.

The project CommuniCity launches 100 tech pilots through 3 Rounds of Open Calls to address the needs of European cities and communities. The goal of the project is to promote technology solutions through co-creation and co-learning processes driven by citizens, designed with and for vulnerable and marginalised communities.

The unique setup of the project objectives requires the use of traditional and specifically tailored data management tools to deal with the wide variety of potential data sources and use. To structure and streamline the presentation of the CommuniCity data management plan, it was decided to do this via the locations where data can be stored.

1. Data Summary

This project is handling data at several levels:

Since the objective of this project is to create a methodology and infrastructure to promote and realise open calls for innovative digital solutions for marginalised communities, most of our information is public, as most of our deliverables have a “public” status.

Of course, organising the open call, collecting proposals and evaluate them implies confidential information that needs within the project protected areas in our platforms to collect and store this information.

The granted pilots are a next level of data concern:

- Depending on the pilot itself, data protection is a concern that is covered via the contract CommuniCity is underwriting with the grand candidate.
- Each pilot however has an obligation to inform and report about results, these reports can only contain public information and can’t reveal personal data of the pilot itself.

Operationally the project has different tools and platforms to store information:

- For the day-by-day project work and preparation of deliverables, Google “shared drive” is used, this drive is accessible for only project collaborators and is password protected.
- For the organisation of the calls (and administrative transactions with the external pilot partners), partner FVH is using “Sales force”, a commercial platform: password protected, GDPR assured.
- For the evaluation of the call and the communication with the jury members, partner FVH is using a own developed platform also password protected.
- What concerns personal, sensitive information used for/collected for the project (surveys, interviews with our sensitive target groups…): this information is stored in a dedicated cloud environment of the University of Amsterdam, the storage is protected by a two-factor authentication procedure. This cloud is managed on servers in the Netherlands by SURF (a cooperative association of Dutch educational and research institutions).
- All public information related to the project is published on the website (https://communicity-project.eu/) and via the social media channels of the project.

2. Open Data Access Policy

2.1 Open and Granular Sharing of Non-Personal Data

For the non-personal data, the project will follow a proactive strategy to make

relevant data:

- **Accessible:** All the data generated by the CommuniCity platform will be freely accessible to all the stakeholders of the platform.
- **Assessable and intelligible:** The data could be used in the future for a scientific purpose, like scientific studies or papers.
- **Usable for secondary purposes:** personal data will be stored for long term preservation and will be exploitable by the tools provided in the context of the CommuniCity project or other tools developed in the future only as long as they are compatible with the initial purposes.
- **Interoperable:** The data provided inside the CommuniCity platform could be exchanged between researchers, institutions, organisations or city authorities using recognised standards.

2.2 Open Access Policy

Where applicable, CommuniCity will follow an open access approach. As stated in the Guidelines on Open Access to Scientific Publications and Research Data: “Open access (OA) refers to the practice of providing online access to scientific information that is free of charge to the end-user and reusable. […] Open access to scientific publications means online access, free of charge, for any user.” The Open Access policy has been supported by key political declarations, such as the 2002 Budapest Declaration and the 2003 Berlin Declaration. Open Access is fully compatible with exploitation, IPR protection and patenting. It exclusively focuses on published information. As stated in the guidelines: “the decision on whether to publish through open access must come after the more general decision on whether to publish directly or to first seek protection.”

Open Access brings several advantages:

- It enables researchers to build on previous research results.

- It encourages synergies, collaborations and avoids duplication of effort.

- It can contribute to accelerate the research process.

- It improves transparency.

CommuniCity will align as much as possible with the “Green” model for Open Access, where “the author, or a representative, archives (deposits) the published article or the final peer-reviewed manuscript in an online repository before, at the same time as, or after publication. Some publishers request that open access be granted only after an embargo period has elapsed.” All articles whose publications are not limited by editor rules will be made available from the CommuniCity website.

2.3 PSI Compliance

The Cities and the other bodies governed by public law will grant open access to the information they hold in accordance with Directive 2003/98/EC, known as the 'PSI Directive', and its national implementing laws. The following principles apply:

• All content that can be accessed under national access to documents laws is in principle re-usable beyond its initial purpose of collection for commercial and non-commercial purposes: by way of exception, content held by museums, libraries and archives is only re-usable if it is made available by the institutions for re-use;

• Re-use of information will be permitted without prejudice to personal data protection, as regulated by Regulation 679/2016;

• Re-use of information will be permitted without prejudice to third parties’ intellectual property rights;

• Conditions for re-use shall be non-discriminatory for comparable categories of re-use;

• Charges for re-use should in principle be limited to the marginal costs of the individual request (reproduction, provision and dissemination costs);

• Exceptions apply to museums, libraries and archives and to situations in which either the public sector body as such is required to generate revenue to cover a substantial part of the costs relating to the performance of its public tasks or situations in which such requirement applies to a specific piece of content ('document');

• In such cases, the charges for re-use must be limited at a ceiling calculated on the basis of actual costs. Public sector bodies need to calculate charges per re-user in a way so that the total income from charging does not exceed the costs incurred to produce and disseminate the information, together with a reasonable return on investment.

• Public sector bodies are encouraged to apply lower charges or to apply no charges at all. On request, public sector bodies must indicate the method used to calculate charges.

• Charges and other conditions for re-use must be pre-established and published. If a request for re-use is refused, the grounds for refusal and the means of redress need to be explained.

• Prohibition of cross-subsidies: If public sector bodies re-use their own documents to offer added-value information services in competition with other re-users, equal charges and other conditions must apply to all of them.

• Prohibition of exclusive arrangements: Public sector bodies may not enter exclusive arrangements with individual re-users, excluding others.

• Two exceptions apply: Exclusive rights may be authorised in exceptional circumstances: (1) if they are necessary to provide services in the public interest or (2) in the context of digitisation of cultural resources.

• In both cases, review clauses ensure that exclusive arrangements are regularly reviewed against the evolution of technology and the market for digitisation and provision of electronic services;

• Requests for re-use shall be processed within a specific timeframe (20 days for standard cases).

• Licences should not unnecessarily restrict possibilities for re-use or be used to restrict competition.

• Where possible, the cities will use standard licences in digital format.

As data are conceived as public and open at the outset, there is no need to have an access committee in place. Should such a necessity arise for data kept by cities or public authorities according to national law, it will be regulated at local level in accordance with the applicable law.

3. FAIR data

Each consortium partner will ensure FAIR (findable, accessible, interoperable, and reusable) data principles where applicable.

3.1 Making data findable, including provisions for metadata

Open access data sources will be discoverable, identifiable and locatable using standard identification mechanisms.

To maximise access to the data, project activity data will be assigned by number of activity (deliverable), project acronym and number, name of file content, date.

To optimise possibilities for re-use and enable findability of CommuniCity data, research publications and information in website/social media will be provided by search keywords. Clear version numbers will be added to each document by each consortium organisation.

3.2 Making data accessible

The project will produce scientific research reports, conference proceedings, presentations, material for social networks, policy reports, monitoring reports, strategy planning documents and other materials that will be disseminated with open publications.

Material which has been limited through non-disclosure agreements with partners and/or governmental institutions, will be confidential.

Dissemination level of project governance plan, risk assessment report, General Assembly feedback, part of information of practical workshop on project proposal preparation and management, media monitoring report is planned to be confidential, available only for members of the consortium.

Knowledge management, ownership and access to key project information will follow best practices principles and be treated accordingly.

Project results intended for public use will be communicated with partner organisations and government institutions.

All articles arising from the CommuniCity project will be published according to the guidelines.

3.3 Making data interoperable

Open access data produced in the CommuniCity project will be interoperable allowing data exchange and re-use. Data will be made available in standard formats compatible with available (open) software applications to enable unrestricted data exchange between cities, institutions, organisations, countries and others.

The following standards and metadata are envisaged:

(1) for Personal data: these data will be minimised, in line with the General Data Protection Regulation. They will be handled accordingly and will not be shared with third parties, but they can be made available for the individual user if they wish to get access to their data. Linkability of Devices and Measurements Data with Personal Data will be avoided and prevented unless it is strictly necessary.

(2) for Devices data: this dataset will be aligned with CKAN and OASC data models (MIMs), to ease the portability and reusability of device profiles.

(3) for Measurements data: this dataset will be aligned with CKAN and OASC data models (MIMs), to ease the portability and reusability of such measurements.

3.4 Increase data re-use

Decision of making data available and re-usable to third parties will be made after communication and agreement with the Consortium member and owner of the data, considering intellectual property rights regulations.

3.4.1 Data sharing

Personal data will allow identification of subjects for data processing aims but for no longer than it is necessary. This will be strictly in accordance with institutional, national and EU law – original personal data and information will not be transferred to third parties without additional permission:

(1) for Personal data: these data will be handled in conformity with the EU General Data Protection Regulation and will not be shared with third parties, except if a legal ground to do so exists, such as if an individual will ask for access to their own data.

(2) for Devices data: this dataset is required for the platform to work and monitor its activity. It will be made available to the different components of the SynchroniCity platform and may appear on the public interface in order to enable the end-users to identify devices to interact with.

(3) for Measurements data: these data will be handled by the platform, but their publication will remain under the control of the tester. Anonymised data may be used by the platform to develop benchmarking and for performance and statistics purpose.

3.4.2 Archiving and preservation

Long term storage of data during the project lifetime is provided by the coordinator and members of Consortium.

The project Coordinator institutions will store the data for five years after the end of CommuniCity project.

Data quality is mainly the responsibility of data creators and assured by project partner organisations, evaluating accuracy, relevancy, completeness, timeliness and consistency.

4. Other research outputs

Special attention must be given for the data output of the pilot projects. The development of Digital tools for vulnerable groups must have our attention what concerns data management but the project as such has only an indirect control on these very diverse and in the context of the project small projects. The consortium tries to handle this issue at different levels:

- Upfront at the selection of the projects: the pilot candidates are informed via the CommuniCity website about the "Key ethical points of piloting and community engagement". Specially action point 8 refers to data usage.
- The evaluation of the proposals in the third call, will take "good practice in data management" as an evaluation criterion.
- Once a project is selected each of the pilot cities have their proper rules for dealing with ethical question as personal data management:
    - The City of Helsinki requires a "Research permit".
    - The city of Amsterdam requires an assessment of their "privacy officer" who can in some cases request a DPIA (Data Protection Impact Assessment).
    - City of Porto/Porto Digital is doing a GDPR check for the selected projects.
- Once a contract is signed between a particular pilot and the city, this contract contains clauses that the pilots need to declare itself in accordance with the European regulation (see annex 1)
- In the mid-term and end-reports the pilots need to report on compliances that concerns data regulations, GDPR and ethical aspects of the project. These reports will be assessed by the External Ethical Board.

5. Allocation of resources

The CommuniCity project assigns a DPO to survey all aspects of data management and protection, this DPO will be supported by the DPO's or privacy officers of the pilot cities which concerns the specific pilot related issues.

6. Data security

All data will be stored and transferred according to applicable national, EU and international legislation for data security regulations. General procedures for data handling, management and storage will be applied.

6.1 Website (including publications)

The current CommuniCity website encrypts all data exchanged between visitors and the webserver.

6.2 Repository

A security/privacy mechanism of the repository is applied.

6.3 Open Calls Platform

The Platform employed in the CommuniCity project will collect data of the applicants, through an online form which will be used during the projects Open Calls. Data will be deposited and secured in the platform and managed by the CommuniCity consortium. The information will be captured through online forms and will be recorded and stored in Cloud infrastructure. The information will be accessible through an online application and only the anonymized data will be downloadable in csv and xls formats. Only authorised users will be allowed to access the data sets via authentication. The platform applies technological and organisational measures to secure processing of personal data against publishing to unauthorised persons, processing in violation of the law and change, loss, damage or destruction. In the project's terms and conditions for data sharing, it is stated that it is not allowed to try and de-anonymize the data sets provided to the project..

The applied platform security measures:

- Registration and logging in to the platform proceed in a secure https connection. Use of password to access data sets: to secure access to data by unauthorised users.
- Options for reading data: the platform offers the possibility to make data available in a read- only or downloadable format, hindering the access to information by unauthorised users. Once an Open Call finishes information is archived, so it’s no longer publicly accessible, only administrators will have access to the historic data in a read-only mode.

- Back-up policy: complete and redundant backups are done on a regular basis. Moreover, every time a modification is done an older version is saved.
- Accidental deletion or modifications: in case of a catastrophic event that implies the partial or complete deletion of the data sets, the data from the most recent backup will be automatically restored (back-up every predefined time period). In case of accidental deletion or modification only the most recent document will be restored, so in case of accidental changes or deletion data can be easily recovered.
- Deletion or modification of data by users: only administrators have the right to delete or modify the information included in the datasets. Under exceptional circumstances, administrators can be given permission to delete applications but the user responsible of its creation will be notified before doing so.
- Deletion of data by participants in open calls: users having started the application process can withdraw any time using the FBA platform before the deadline for submission.
- Terms and conditions: the platform has specific terms of use and conditions that must be accepted by all users of the platform.

Each partner is responsible for all obtained data during their processing and acquisition in their organisation. Each partner is obliged to implement appropriate security measures to ensure the confidentiality of the data. Each partner must keep on file detailed information on the informed consent procedures regarding data processing and templates of the informed consent forms and information sheets.

6.4 Matchmaking tool

Access to “CommuniCity Matchmaking tool” platform end-to-end secured is used to ensure use by humans.

Users are allowed to submit a New Search to the “CommuniCity Matchmaking tool” without registration by providing their “Email address” and “Full Name” information in the “Message Board” provided.

7. Ethics

A specific Work Package (WP2) will deal with "Ethical and Inclusive Engagement in Practice" and an External Ethics Advisory Board has been set up to monitor and guide implementation of ethical issues in the project. This External Ethics Advisory Board will produce a yearly report. The first report delivered November 2023 made an ethical screening of the relevant deliverables produced the first year of the project and a screening of the potential risk factors on ethics, data privacy aspects of the first 13 pilots (results of the first round of call).

As part of the engagement on ethics, the CommuniCity consortium has been committed to ensuring that ethical principles are applied in the scope of the activities performed in the project from the beginning to the end and to ensure that all the activities of the project are compliant with the ethical standards of EC.

CommuniCity will also take care that the Pilots selected through the Open Calls apply to the ethical standards and guidelines of Horizon 2020. The External Ethics Advisory Board will review the Open Call phases, the pilots selected, subject them to strict ethical screening/requirements on personal data protection and any other potential ethical issues. If any project seems to have Ethical issues the Committee will indicate the specific actions to be taken and will participate in the monitoring sessions of these projects during the entire project life cycle. Additionally, a series of Key ethical points of piloting and community engagement have been produced by the University of Amsterdam (WP2 - Ethical and Inclusive Engagement in Practice):

- Your pilot should be centered around the needs of vulnerable and marginalised communities.
- While working with the communities, the 'do no harm' principle is at the core of all engagement activities.
- Your social skills matter.
- We value creating AI and broader technological solutions with and for the communities rather than 'testing' the solutions on their members.
- Co-creation also applies to the relation between tech provider and association.
- We believe in Fair AI (MIM5).
- Transparency and explainability matter, as well as privacy, data protection and responsible data use.
- We aim to learn from this project together. We want to learn from both our successes and failures.

- Responsibility and accountability are among the core values while engaging with vulnerable and marginalised communities. This engagement should be mutually rewarding.
- Open mind and flexibility will be needed while piloting: you will be collaborating with people with diverse backgrounds, also in a professional sense – beyond the AI/technological world, we are civil servants, managers, researchers, social innovation experts, and the list continues.

8. Conclusions

The first version of the Data Management Plan gives a status of the project after the first year of activity behind and the experience of the first pilot round and the second call launch.

The main learnings of this first year is that the project must integrate date awareness and the FAIR data principles into the framework of the 3rd call in a way that the project and the tools it delivers delegate these responsibilities in the right way towards the pilot cities and pilots in a “cascading” flow.

Since the project has as main objective to develop a methodology and infrastructure for piloting digital solutions for vulnerable and marginalised communities, these data management aspects at the pilot level and how to handle these in the context of large-scale calls needs to be the focus of the second Data Management Plan at the end of the CommuniCity project.

Lessons learned for the Third Call:

- The CommuniCity DPO and the DPO’s of the pilot cities supervise the call proposals and the selected pilots itself.
- Good practice in Data management will be an evaluation criterion in the 3rd call.
- Each selected project had to present a data management assessment in its mid-term and final report.
- Data protection will be an obligatory article in the project's contract.
- Data protection will be a specific item in the pilot manual documentation and in the kick-off meetings of the project.

Annex 1

Citation out of the pilot contract (Annex 4) about data and data protection:

The Supplier must process personal data under the Contract in compliance with the applicable EU, international and national law on data protection (in particular, Regulation 2016/6796). The Supplier shall be acting as processor and in this role shall process personal data on behalf of the Client, acting as controller. The Supplier must ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subjects

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- accurate and, where necessary, kept up to date

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed and

- processed in a manner that ensures appropriate security of the data.

The Supplier may grant their personnel access to personal data only if it is strictly necessary for implementing, managing and monitoring the Contract. The Supplier must ensure that the personnel is under a confidentiality obligation.

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 ('GDPR') (OJ L 119, 4.5.2016, p. 1).

CommuniCity

This project has received funding from the European Union's Horizon Europe research and innovation action HORIZON-CSA under the grant agreement No 101070325 (Communicity). This deliverable reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.