Co-inform

Context Matters,
Your Sources Too

Data Management Plan

D7.1

#ThinkCheckShare

Document Summary Information

Project Title:	Co-Inform: Co-Creating Misinformation-Resilient Societies		
Project Acronym:	Co-Inform	**Proposal Number:**	770302
Type of Action:	RIA (Research and Innovation action)		
Start Date:	01/04/2018	**Duration:**	36 months
Project URL:	http://coinform.eu/		
Deliverable:	D7.1 Data Management Plan		
Version:	1.1 Final version		
Work Package:	WP7		
Submission date:	7/10/2018		
Nature:	Report (RE)	**Dissemination Level:**	Public (PU)
Lead Beneficiary:	Stockholm University		
Author(s):	Vasilis Koulolias, eGovlab, Director (SU) Cecilia Magnusson, Professor Department of Law (SU) Oxana Casu, Project Manager (SU) Dimitris Sotirchos, Project Assistant (SU)		
Contributions from:	All Co-Inform Consortium Partners (UKOB, FCNI, IHU, IIASA, OU, Scytl, ESI, CUT)		

The Co-inform project is co-funded by Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) H2020-SC6-CO-CREATION-2016-2017 (CO-CREATION FOR GROWTH AND INCLUSION).

Revision History

Version	Date	Change editor	Description
v1.0	16/08/2018	SU	Initial Draft
v1.1	6/09/2018	SU	First Review
v2.0	29/09/2018	All Co-Inform Consortium Partners	Review Integration and further editing
v2.1	1/10/2018	All Co-Inform Consortium Partners	Second review integration and further comments addressed
v2.2	5/10/2018	SU, ESI	Peer review integration
v3.0	7/10/2018	SU	Final version

Disclaimer

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Union. Neither the Co-Inform Consortium nor the European Commission are responsible for any use that may be made of the information contained herein.

Copyright Message

Executive Summary

This Data Management Plan will describe how the project handle data. Co-Inform intents to comply with the General Data Protection Regulation (GDPR). Therefore, it has set out guidelines for the consortium on how to safely and securely handle sensitive data. The Project Management has developed provisional guidelines on how to implement the FAIR principles to the datasets.

Table of Contents

1. Introduction 7
2. Objectives 9
2.1 Types of data that the project will generate/collect 9
2.2 Origin of the data 10
2.3 Expected format of the data 10
3. Data Management and the GDPR 11
3.1 Lawfulness, fairness and transparency 11
3.2 Purpose limitation 11
3.3 Accuracy 11
3.4 Storage limitation 12
3.6 Integrity and confidentiality 12
3.7 Accountability 12
4. Guidelines for data management on project level 13
4.1 Purpose limitation and data minimization 13
4.2 Personal information 13
4.3 Anonymization and pseudonymization 13
4.4 Informed consent 14
4.5 End users' access to data 14
4.6 Storage and researchers' access to data 14
4.7 Security Updates and Best Practices 15
4.8 Responsibility and compliance 15
4.9 Encryption 16
4.10 Open data and FAIR principles 16
4.11 Privacy statements 16
4.12 Update the DMP document 16
5. Ethical and legal aspects 17
6. Data management per WP 17
6.1 Data for WP1 Co-Creation of Community and Culture 17
6.2 Data for WP2 Co-Creation of Misinformation Management Policies 19
6.3 Data for WP3 Big Data Intelligence 21
6.4 Data for WP4 Agile Development of Misinformation Resilience Platforms 23

6.5 Data for WP5 Assessment of effect on misinformation-related practices and policies 25
6.6 Data for WP6 Dissemination, Exploitation, and Communication 27
6.7 Data for WP7 Management 29
ANNEX 1 31

Abbreviations and Acronyms

CUT	Cyprus University of Technology
DM	Data Manager
DMP	Data Management Plan
FAIR	Findable, Accessible, Interoperable, Re-usable
GDPR	General Data Protection Regulation
OU	Open University
SSL	Secure Sockets Layer
SU	Stockholm University
UKOB	University of Koblenz-Landau
USB	Universal Serial Bus
VPN	Virtual Private Network
WP	Work Package

1. Introduction

Co-Inform is about empowering citizens, journalists, and policymakers with co-created socio-technical solutions, to increase resilience to misinformation, and to generate more informed behaviors and policies. The aim of Co-Inform is to co-create these solutions, with citizens, journalists, and policymakers, for (a) detecting and combating a variety of misinforming posts and articles on social media, (b) supporting, persuading, and nourishing misinformation-resilient behavior, (c) bridging between the public on social media, external fact checking journalists, and policymakers, (d) understanding and predicting which misinforming news and content are likely to spread across which parts of the network and demographic sectors, (e) infiltrating echo-chambers on social media, to expose confirmation-biased networks to different perceptions and corrective information, and (f) providing policymakers with advanced misinformation analysis to support their policy making process and validation.

To achieve these goals, Co-Inform will bring together a multidisciplinary team of scientists and practitioners, to foster co-creational methodologies and practices for engaging stakeholders in combating misinformation posts and news articles, combined with advanced intelligent methods for misinformation detection, misinformation flow prediction, and real-time processing and measurement of crowds' acceptance or refusal of misinformation. Co-Inform tools and platform will be made freely available and open sourced to maximise benefit and reuse. Three main stakeholder groups will be directly engaged throughout this process; citizens, journalists, and policymakers.

This document is the Co-Inform data management plan (DMP). The DMP describes the data management life cycle for all datasets to be collected, processed and/or generated by the research project. The H2020 DMP describes, among others:

- The handling of research data during and after the project
- The type of data that will be collected, processed, or gathered
- What methodology and standards will be applied?
- Whether and how the data will be made (openly) accessible
- How the data is stored

The procedures described shall be followed by all members of the Consortium and ensure that data on participants are transferred and used in a secure setting; that use of the data is compliant with ethical and legal requirements. This includes signed informed consent (i.e. legitimate consent) a template is provided in Annex 1, ethics approval, and applicable data protection laws. The use of both existing as well as new data occurs in agreement with the Data Owner/Data Provider. Management of datasets that include personal information of study participants will also be compliant with the General Data Protection Regulation (GDPR, (EU) 2016/679).

This Data Management Plan (DMP) is the first deliverable in the seventh Work Package (WP7) of the Co-Inform project. It will describe how the data will be handled during and after the project. After the project has ended the focus will shift towards making the data as openly accessible as possible. By means of anonymizing the personalized data, the consortium will try to open up as much data as possible.

In this document, initially, objectives of the document will be described. Then, the relationship between the GDPR and the implementation of data management within the Co-Inform project will be discussed. In the chapter 4, guidelines will be provided for the partners within the consortium on working with datasets that contain personal information.

2. Objectives

In this deliverable the data management of the Co-Inform Project will be described. Discussions on Privacy by Design and Open Data will be ongoing during the project.

The aim for the DMP is to be a description of the datasets within the Co-Inform project, but also to provide guidelines for data management to all partners in the project. The DMP can also serve as a tool to create awareness on the different topics of Open Access, Privacy and Personal Data, and the FAIR principles (Findable, Accessible, Interoperable, Re-usable). This will help the participants to make as much of the research data Openly Accessible as possible, while staying within the boundaries of the Privacy regulations. Thus, the DMP will not only support formal compliance with regulatory frameworks but also general data protection principles.

The purpose of data collection in the Co-Inform project is to advance the state of the art in understanding misinformation dynamics by studying how different demographics (particularly age, gender and geographical location) and user behaviour, as well as different topologies and typologies of the social networks influence the spread of misinformation. Based on this understanding, Co-Inform will propose models for accurately predicting misinformation flow. The data collection will comply with all national and EU ethics and legal requirements. Access to use these data is needed to address the different Co-Inform objectives as specified in the grant agreement and summarised below:

- Objective 1: Acquire stakeholders' socio-technical requirements and values with regards to misinformation.
- Objective 2: Co-create, implement, and test policies for managing misinformation.
- Objective 3: Develop intelligent big data technologies to automatically identify misinformation content and sources, and relevant corrective information.
- Objective 4: Develop intelligent big data technologies to understand and predict patterns of misinformation flow on social networks.
- Objective 5: Develop an intelligent platform for misinformation awareness and resilience.
- Objective 6: Support informed policy generation with advanced misinformation analysis.
- Objective 7: Measure and monitor citizens’ perceptions and behaviour with regards to processing and sharing misinformation.

2.1 Types of data that the project will generate/collect

Co-Inform will collect data from several sources:

- 3rd party websites (e.g. data libraries, news media, NGOs) and open and public social media (e.g. Facebook, Twitter)
- Live data from Pilots that will take place in Austria, Greece and Sweden.
- Surveys and questionnaires from user studies (quantitative data)
- End-user interviews (qualitative data)

In addition to the above, secondary data (or information) will be generated through analysis and interpretation. More details are provided on how this data will be processed and handled is provided **in below sections.**

2.2 Origin of the data

The origin of the data will come from:

- Academic research
- Surveys and questionnaires (accompanied by informed consent)
- Social media datasets (open and public data)
- Publicly accessible websites
- Workshops (informed consent)

2.3 Expected format of the data

All data used in project must use non-proprietary formats using standard representations (Unicode) and meet the following requirements:

1. Non-proprietary
2. Open, documented standard
3. Common usage by research community
4. Standard representation (ASCII, Unicode)
5. Uncompressed

Collected data will be converted to commonly used and parsable formats (e.g., XML, JSON). To whom might it be useful (**'data utility'**)?

- Co-Inform consortium
- European Commission services and European Agencies
- EU National Bodies
- The general public including the broader scientific community
- Fact-checking organisations.

3. Data Management and the GDPR

The introduction of GDPR in May 2018 means that all partners within the consortium will have to follow the same new rules and principles. This makes it easier for the project management to set up guidelines for the correct use of personal data.

In this chapter will be described how the basic principles of the GDPR will be followed in the Co-Inform project. In the next chapter we will set out specific guidelines for proper use of personal data within the boundaries of the GDPR. Co-Inform describes all handling of personal data in this DMP. Some of the answers requested at the moment of writing cannot be provided for. Therefore, we chose to let the DMP be a living document. As soon as information about data sets become available, this will be updated in the DMP.

3.1 Lawfulness, fairness and transparency

All data gathering from individuals will require informed consent of the participants who engage in the project. Informed consent requests will consist of an information letter and a consent form. This will state the specific causes our project activities, how the data will be handled, safely stored, and shared. The request will also inform individuals of their rights to have data updated or removed, and the project's policies on how these rights are managed. Further consent will be asked to use the data for open research purposes, this includes presentations at conferences, publications in journals as well as depositing a data set in an open repository at the end of the project.

The consortium will be as transparent as possible in their collection of personal data. This means when collecting the data information leaflet and consent form will describe the kind of information, the way in which it will be collected and processed, if, how, and for which purpose it will be disseminated and if and how it will be made open access. Furthermore, the participants will have the possibility to request what kind of information has been stored about them and they can request up to a reasonable limit to be removed from the results.

3.2 Purpose limitation

The Co-Inform project won't collect any data that is outside the scope of the project. Each researcher will only collect data necessary within their specific work package.

3.3 Accuracy

All data collected will be checked for consistency. However, since some of the dataset register self-reporting data from participants, this data cannot be checked for accuracy. Since all data is gathered within a specific timeframe, it is chosen not to keep the data up to date, since it would hinder our research.

3.4 Storage limitation

All personal data that will no longer be used for research purposes will be deleted as soon as possible. All personal data will be made anonymous as soon as possible. At the end of the project, if the data has been anonymized, the data set will be stored in an open repository. If data cannot be made anonymous, it will be pseudonymized as much as possible and stored for a maximum of the partner's archiving rules within the institution.

3.6 Integrity and confidentiality

All personal data will be handled with appropriate security measures applied. This means:

- All data sets will be stored with security constraints that include password protection, encryption and other access restrictions to IT systems and storage that comply with Swedish law and the EU's applicable regulatory framework.

- All data sets will be stored on encrypted disk drives on servers located at the Department of Computer and Systems Science at Stockholm University (DSV) of Stockholm University that complies with all GDPR regulations.

- Physical access to project servers is limited to security-based IT staff only, and access to data over the Internet will be limited to research consortium researchers via secure virtual private network VPN.

- These data files cannot be copied, unless stored encrypted on a password protected storage device. In case of theft or loss, these files will be protected by the encryption.

- These copies must be deleted as soon as possible and cannot be shared with anyone outside the consortium or within the consortium without the proper authorization.

In exceptional cases where the dataset is too large, or it cannot be transferred securely, each partner can share their own datasets through channels that comply with the GDPR.

3.7 Accountability

At project level, the project management is responsible for the correct data management within the project. In the next chapter, guidelines will be described for each partner to follow in case of datasets with personal data. Whether the partners follow these guidelines will be regularly checked by the project management. For each data set, a responsible person has been appointed at partner level, who will be held accountable for this specific data set. Each researcher will need to make a mention of a dataset with personal information to their Privacy Protection Officer, in line with the GDPR regulations.

4. Guidelines for data management on project level

Data management is an ongoing process. For many tasks, due to the nature of the research, we do not know what kind of data we will collect specifically. Therefore we have established guidelines for data management to ensure that all researchers will keep up the principles of lawful and ethical data management.

The guidelines established in this DMP are embraced within the consortium and the project management will ensure these principles will be followed.

The sections below describe the ten basic guidelines that will be adopted in the Data Management process in Co-Inform.

4.1 Purpose limitation and data minimization

As soon as a researcher has identified which information to collect, the principles of purpose limitation and data minimization come into play. Each researcher will take care not to collect any data that is outside the scope of his or her research and will not collect additional information not directly related to the goal of his research

4.2 Personal information

As soon as the parameters in the data set are identified, the researchers need to indicate whether the data set will contain personal information. In cases where the parameters themselves contains no personal information, but the various parameters can be merged to show a distinct pattern that can be linked to a specific person, the data set will be classified as containing personal information as well.

When the dataset contains personal information or otherwise information that needs to be kept confidential, the following privacy principles should be taken into account: Sensitive data should be stored at the dedicated secure cloud at the Computer Science Department (DSV).

In the case of personal data collected in physical form (e.g. on paper), it shall be stored in a restricted access area (e.g. locked drawer) where only designated staff have access to. When the data has been digitized, the physical copies will have to be removed. Personal data should be deleted as soon as possible.

4.3 Anonymization and pseudonymization

All researchers will make sure that personal data is anonymized (i.e. personally identifiable fields will be replaced such that participants cannot be identified, and thus GDPR is no longer applicable) as quickly as possible. When the data cannot be anonymized completely, it will be pseudonymized as much as possible. The key between the pseudonymized file and the list of participants will be stored by the project management on a separate physical location from the original files. Research subjects should be able to withdraw their data within 48 hours of the research activity carried out. Furthermore, the Data Manager will keep an audit log of all partners who have requested and hold a copy of the anonymized dataset to ensure the data is processed according to the purpose for which the data was collected.

4.4 Informed consent

Data published on public social media will be collected and processed without anonymization, given that they are publicly shared and accessed. However, data from social media will not be republished without full anonymization (still personal data), and in accordance with the terms and conditions of the said social media platform. Data from interviews and surveys will be fully anonymized (no longer personal data) before they are shared with Co-Inform partners, unless the data provides have explicitly given his/her consent to using the data without anonymization. The data will not be released to any third party and will not be transferred to countries outside the EU. When collecting personal information, researchers are required to get informed consent from the participants. An informed consent form template is provided in Annex 1**.**

Dissemination of information for scientific conferences, journal papers or other dissemination items may only occur after any personal data is completely anonymized, otherwise informed consent will be sought there too.

The collected data will be stored on secure encrypted drives on servers hosted by project partners. While physical access to these servers will be restricted to only security cleared IT staff, online access to the data will be restricted to individual members of project and will use encrypted SSL communication channels.

The Data Manager will monitor and maintain audit log to keep track of all the datasets that are shared with project partners and its members. Participants can withdraw their consent at any stage of the study and request that their data be destroyed from the system.

4.5 End users' access to data

The user can submit a request to see which information about him is being kept on our files through the contact person on the consent form. Furthermore, he can request that no additional data collection of the participant will take place starting immediately from the time of request.

4.6 Storage and researchers' access to data

If and when personal data is collected, it will be stored on access restricted secure server. We will use physical server protection including access restrictions in a locked server room. Only authorized and professional IT system administrators will be allowed to have physical access to the servers. The server rooms hosting the physical servers will have the following facilities:

1. Multilevel access control
2. Fire protection
3. Climate control system
4. Redundant power supplies
5. Encrypted communication channels

Specifically, these will be the encrypted disk drives on servers located at the Department of Computer and Systems Science (DSV) of Stockholm University or a partner's own solution that complies with the GDPR. Access to all data requires an authenticated user. The private keys of encrypted drives which store them, will be available only to the project members. Similarly, access to private keys which are used in the transmission of data will be restricted to project members.

In all cases, the Data Manager (DM) will administer the access to these private keys (both storage and transmission). It is the partners' responsibility to ensure that this data is not stored on unencrypted mobile devices (e.g., CDs, USB sticks) or unsecured web servers.

Furthermore, we will use SSL connections and use secure passwords, and restrict connections to the organizations' subnets (or provide access via VPN). Co-Inform will use encrypted connections and not allow access to database servers from unknown workstations. Access to this secure environment can be granted or revoked by either the researchers responsible for the data, or the project management on a case to case basis and will not be given out by default to all researchers. All users that are granted access will need to sign a confidentiality agreement about the data on the server. Access can also be restricted or revoked, when researchers are not complying with the guidelines or when their contract is terminated.

4.7 Security Updates and Best Practices

We will automatically deploy security updates and subscribe to all relevant security mailing lists. The storage of (parts of) the collected data on mobile storage devices (e.g., USB sticks, CDs) at high risk of being lost/stolen will be avoided.

All servers will be updated on a regular basis to ensure known vulnerabilities or exploits will not compromise the system.

In addition to that the system administrators follow security blogs to ensure to keep updated with the latest recommendation for securely configuring all provided services.

4.8 Responsibility and compliance

All project partners and their team members are expected to comply with this data management strategy including related legislation. Potential new team members will be fully informed about this strategy and requested to adopt all its rules before starting their work in the team. The Data Manager will periodically (at least once a year) review the compliance of this data management plan with the project partners and implement corrective measures if required.

4.9 Encryption

When you want to share personal data files, the data files will need to be encrypted. Each researcher is free to use their own preferred encryption tools, to make the process as easily available as possible. Possibilities for encryption as build in Word and Excel encryption or PGP keys.

4.10 Open data and FAIR principles

Within the Co-Inform project, we endorse the EC's motto: to make the data as open as possible, but as closed as necessary. We are committed to protect the privacy of the people involved, and the confidentiality of specific results or agreements. In these cases, the data will not be made available for public use. In all other cases we will try our best to make the research data as broadly available as possible. This means the FAIR principles will be held, but at the moment it is not possible for us to give definitive answers on how these will be held. We intent to discuss those in more detail, when we receive additional information on the data sets.

4.11 Privacy statements

Actively communicate the privacy and security measures you take through all media channels (from consent forms to websites) with a privacy statement. You can adjust the statement to fit the target group, purpose, and level of privacy.

4.12 Update the DMP document

The DMP is a living document. The fact that at the moment there are still many uncertainties about the data that will come up in future research does not release us of the obligation to ethically and lawfully collect, process, and store this data. All researchers have the responsibility to keep the DMP up to date, so the DMP will reflect the latest developments in data collection.

5. Ethical and legal aspects

There are ethical as well as legal aspects that will be taken into consideration both proactively and reactively. Ethical or legal issues that can have an impact on data sharing are discussed more extensively in the ethics review. Governing legislation (in a broad sense) concerns primarily compliance with GDPR (see above) and supplementary national laws, if such exist at all. In addition, there are rules and regulations applicable in the public sector of Sweden concerning for instance, rights of access (openness/transparency), records management for archival purposes and administrative procedures; all of which the project is aware of.

6. Data management per WP

The work package leaders have been asked to describe the different data sets that will be used within their WP as well as possible. For the description of the work packages the standard EC template for a data management plan has been used. However, many questions concerning metadata and the FAIR principles cannot be answered at this stage of the project. If not otherwise specified in the Work Package description, the above general guidelines will for now apply to the data set.

6.1 Data for WP1 Co-Creation of Community and Culture

1. Data Summary

The purpose of Data Collection in this WP is initially to establish a co-creation framework through workshops and jam sessions in order to collect socio-technical requirements from stakeholders. The goal is to then use these requirements to organize the Pilots and develop the platform working with all WPs. The pilots aim to closely and regularly engage with stakeholders, in real-world scenarios and environments, to co-create. Interviews, surveys, and multiple co-creation workshops with citizens, journalists, and policymakers will help the consortium collect the required data.

The following datasets are being collected:

- Notes and minutes of brainstorms and workshops (.doc format)
- Video, audio recordings and notes from interviews with stakeholders (.mps, .doc, MP3, MPEG or AVI. format)
- Transcribed notes/recordings or otherwise ‘cleaned up’ or categorized data. (.doc, .xls format). The files are initially stored as word and excel files. If it is possible to anonymize them and can be used for open access, these files will be stored in the equivalent Open Office format or as pdf.

- Recordings and notes from internal Consortium meetings via the Blue Jeans teleconference software, after participants consent, subsequently uploaded into the Basecamp project management software (used for internal communication and with restricted access only for project partners).

No data is being re-used. The data will be collected/generated by Co-Inform Consortium researchers before during, or after project meetings and through interviews with stakeholders. All data gathering will take place within the EU.

FAIR Data 2.1. Making data findable, including provisions for metadata

At this stage of the project metadata issues still remain open. Metadata-related information will be added during and at the end of the project in line with metadata conventions. All data files will be named so as to reflect clearly their point of origin in the Co-Inform project structure as well as their content. No further deviations from the intended FAIR principles are foreseen at this point.

2.2 Making data openly accessible

Depending on the answers the participants will give, the dataset might contain personal information. The answers might contain personal information related to the subject’s age, gender, professional position, etc. If it turns out the dataset does contain personal information, then it will be treated in line with the project’s guidelines. Microsoft Office should be sufficient to open the document and spreadsheet files. We foresee no restrictions to the dataset, if and when completely anonymized. No further deviations from the intended FAIR principles are foreseen at this point.

2.3. Making data interoperable

By storing the data in Microsoft Office format, these data files can be read by non-commercial administrative tools, like Open Office as well. In case MP3 files will be recorded, these are universal and can be played through multiple software tools. The collected data will be ordered so as to make clear the relationship between questions being asked and answers being given. It will also be clear to which category the different respondents belong (consortium members, external stakeholder). The data will use common social science data collection practice. One potential deviation in terms of privacy has to do with whether the answers will contain personal information. No further deviations from the intended FAIR principles are foreseen at this point.

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

The data will be stored in a trusted repository. At the moment, there is no intention for patenting the information. By posting the data in an open repository such as MySQL, we will ensure that the data will be made available for re-use. Only the final data set will be submitted in the repository. No further deviations from the intended FAIR principles are foreseen at this point.

3. Allocation of resources

The work to be done in making the data FAIR will be covered by the ordinary working budget for producing the deliverables.

4. Data security

Workshop and interview data will be gathered in the form of notes and audio recordings. Audio recordings and handwritten notes will be stored under lock in the offices of the Department of Computer and Systems Science (DSV) of Stockholm University in a physical storage space separate from the participant lists of workshops and interviewees. Audio recordings and handwritten notes will be destroyed once they have been added to the typed notes from the workshops or interviews. In cases where audio recordings or handwritten notes are never added to the typed notes, they will be destroyed in any case no later than the end of the Co-Inform project. Typed notes (i.e. files in word or excel format) will be stored on encrypted disk drives on servers at the Department of Computer and Systems Science (DSV) of Stockholm University. Access will be granted in line with the project's procedures.

5. Ethical aspects

All workshop participants and interviewees will be asked to sign a consent form giving consent to use of the data in the Co-Inform project's analyses and for the sharing of the data with others through FAIR measures. Consent for the two different uses will be specific. Consenting to the use of collected data for the purposes of the Co-Inform project's analyses will be a mandatory requirement for workshop participation and the conduct of interviews. In cases of non-consent to FAIR use of the data, the statements produced by the person in question will be marked with a non-personal marker and eliminated from the dataset before publication. If and when during data collection, there is any possibility of identifying individuals through their responses, the specific data will be treated as personal data and will be stored in line with the project's guidelines

6. Other

No other procedures are required to be put in place for project management data.

6.2 Data for WP2 Co-Creation of Misinformation Management Policies

1. Data Summary

The purpose of Data Collection in this WP is to gather policy requirements from stakeholders (journalists, policymakers and citizens) to guide the management of misinformation in Co-Inform. The main work is focused on defining and setting up a set of policies and rules that Co-Inform processes should follow to autonomously handle identified misinformation.

The following datasets are being collected:

- Notes and minutes of brainstorms and workshops (.doc format)
- Recordings and notes from interviews with stakeholders (.mps, .doc format)
- Transcribed notes/recordings or otherwise ‘cleaned up’ or categorised data. (.doc,.xls format). The files are initially stored as word and excel files. If it is possible to anonymise them and can be used for open access, these files will be stored in the equivalent Open Office format or as pdf.

No data is being re-used. The data will be collected/generated by Co-Inform Consortium researchers before during, or after project meetings and through interviews with stakeholders. The data will be collected/generated by UKOB and Partners through interviews or surveys with stakeholders. All data gathering will take place within the EU.

FAIR Data 2.1. Making data findable, including provisions for metadata

At this stage of the project metadata issues still remain open. Metadata-related information will be added during and at the end of the project in line with metadata conventions. All data files will be named so as to reflect clearly their point of origin in the Co-Inform project structure as well as their content. No further deviations from the intended FAIR principles are foreseen at this point.

2.2 Making data openly accessible

Depending on the answers the participant will give, the dataset might contain personal information. The answers might contain personal information related to the subject’s age, gender, professional position, etc. If it turns out the dataset does contain personal information, than it will be treated in line with the project’s guidelines.
Open Office should be sufficient to open the document and spreadsheet files.
We foresee no restrictions to the dataset, if and when completely anonymized.
No further deviations from the intended FAIR principles are foreseen at this point.

2.3. Making data interoperable

By storing the data in Open Office format, these data files can be read by commercial administrative tools, like Microsoft Office as well. In case MP3 files will be recorded, these are universal and can be played through multiple software tools. The collected data will be ordered so as to make clear the relationship between questions being asked and answers being given. It will also be clear to which category the different respondents belong (consortium members, external stakeholder). The data will use common social science data collection practice. One potential deviation in terms of privacy has to do with whether the answers will contain personal information. No further deviations from the intended FAIR principles are foreseen at this point.

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

The data will be stored in a trusted repository with an Open Access license. At the moment, there is no intention for patenting the information. By posting the data in an open repository with the Data Seal of Approval, we will ensure that the data will be made available for re-use. Only the final data set will be submitted in the repository. No further deviations from the intended FAIR principles are foreseen at this point.

3. Allocation of resources

The work to be done in making the data FAIR will be covered by the ordinary working budget for producing the deliverables.

4. Data security

Workshop and interview data will be gathered in the form of notes and audio recordings. Audio recordings and handwritten notes will be stored under lock in the offices of the Department of Computer and Systems Science (DSV) of Stockholm University in a physical storage space separate from the participant lists of workshops and interviewees. Audio recordings and handwritten notes will be destroyed once they have been added to the typed notes from the workshops or interviews. In cases where audio recordings or handwritten notes are never added to the typed notes, they will be destroyed in any case no later than the end of the Co-Inform project. Typed notes (i.e. files in word or excel format) will be stored on encrypted disk drives on servers at the Department of Computer and Systems Science (DSV) of Stockholm University. Access will be granted in line with the project's procedures.

5. Ethical aspects

All workshop participants and interviewees will be asked to sign a consent form giving consent to use of the data in the Co-Inform project's analyses and for the sharing of the data with others through FAIR measures. Consent for the two different uses will be specific. Consenting to the use of collected data for the purposes of the Co-Inform project's analyses will be a mandatory requirement for workshop participation and the conduct of interviews. In cases of non -consent to FAIR use of the data, the statements produced by the person in question will be marked with a non-personal marker and eliminated from the dataset before publication. If and when during data collection, there is any possibility of identifying individuals through their responses, the specific data will be treated as personal data and will be stored in line with the project's guidelines.

6. Other

No other procedures are required to be put in place for project management data.

6.3 Data for WP3 Big Data Intelligence

1.Data Summary

The goal of this WP is to produce novel analysis methods and services for the accurate detection, monitoring, and prediction of misinformation from big data. Therefore, data will be collected and integrated from multiple online sources such as social media, blogs, and relevant news sources, as well as data from fact checking websites.

The following datasets are being collected:

- Data from online sources publicly available.
- Notes and minutes of brainstorms and workshops (.doc format)

- Video, audio recordings and notes from interviews with stakeholders (.mps, .doc, MP3, MPEG or AVI. format).
- Transcribed notes/recordings or otherwise ‘cleaned up’ or categorised data. (.doc, .xls format). The files are initially stored as word and excel files. If it is possible to anonymise them and can be used for open access, these files will be stored in the equivalent Open Office format or as pdf.
- User-related logs: Information from user logs will be useful to monitor the user-system interaction.

For data that is publicly available, we comply with the social media’s privacy policy that governs the use of such data. For customised applications which will be deployed within social media (i.e. Facebook) to collect data, we will use the social media platform’s permission system. Data published on public social media will be collected and processed without anonymisation, given that they are publicly shared and accessed. However, data from social media will not be republished without full anonymisation, and in accordance with the terms and conditions of the said social media platform. No data is being re-used. The data will be collected/generated by Co-Inform Consortium researchers before during, or after project meetings and through interviews with stakeholders. The data will be collected/generated by OU and Partners through interviews or surveys with stakeholders.

FAIR Data 2.1. Making data findable, including provisions for metadata

At this stage of the project metadata issues still remain open. Metadata-related information will be added during and at the end of the project in line with metadata conventions. All data files will be named so as to reflect clearly their point of origin in the Co-Inform project structure as well as their content. No further deviations from the intended FAIR principles are foreseen at this point.

2.2 Making data openly accessible

Depending on the answers the participants will give, the dataset might contain personal information. The answers might contain personal information related to the subject’s age, gender, professional position, etc. If it turns out the dataset does contain personal information, then it will be treated in line with the project’s guidelines.
Open Office should be sufficient to open the document and spreadsheet files.
We foresee no restrictions to the dataset, if and when completely anonymized.
No further deviations from the intended FAIR principles are foreseen at this point

2.3. Making data interoperable

By storing the data in Open Office format, these data files can be read by commercial administrative tools, like Microsoft Office as well. In case MP3 files will be recorded, these are universal and can be played through multiple software tools. The collected data will be ordered so as to make clear the relationship between questions being asked and answers being given. It will also be clear to which category the different respondents belong (consortium members, external stakeholder).The data will use common social science data collection practice. One potential deviation in terms of privacy has to do with whether the answers will contain personal information.
No further deviations from the intended FAIR principles are foreseen at this point.

2.4. Increase data re-use (through clarifying licences)
The data will be stored in a trusted repository with an Open Access license. At the moment, there is no intention for patenting the information. By posting the data in an open repository with the Data Seal of Approval, we will ensure that the data will be made available for re-use. Only the final data set will be submitted in the repository. No further deviations from the intended FAIR principles are foreseen at this point.
3. Allocation of resources
The work to be done in making the data FAIR will be covered by the ordinary working budget for producing the deliverables.
4. Data security
Workshop and interview data will be gathered in the form of notes and audio recordings. Audio recordings and handwritten notes will be stored under lock in the offices of the Department of Computer and Systems Science (DSV) of Stockholm University in a physical storage space separate from the participant lists of workshops and interviewees. Audio recordings and handwritten notes will be destroyed once they have been added to the typed notes from the workshops or interviews. In cases where audio recordings or handwritten notes are never added to the typed notes, they will be destroyed in any case no later than the end of the Co-Inform project. Typed notes (i.e. files in word or excel format) will be stored on encrypted disk drives on servers at the Department of Computer and Systems Science (DSV) of Stockholm University. Access will be granted in line with the project’s procedures.
5. Ethical aspects
All workshop participants and interviewees will be asked to sign a consent form giving consent to use of the data in the Co-Inform project’s analyses and for the sharing of the data with others through FAIR measures. Consent for the two different uses will be specific. Consenting to the use of collected data for the purposes of the Co-Inform project’s analyses will be a mandatory requirement for workshop participation and the conduct of interviews. In cases of non -consent to FAIR use of the data, the statements produced by the person in question will be marked with a non-personal marker and eliminated from the dataset before publication. If and when during data collection, there is any possibility of identifying individuals through their responses, the specific data will be treated as personal data and will be stored in line with the project’s guidelines.
6. Other
No other procedures are required to be put in place for project management data.

6.4 Data for WP4 Agile Development of Misinformation Resilience Platforms

1.Data Summary

The goal of this WP is to provide the agile design, development, and deployment of the Co-Inform platforms. This WP's main focus will be to implement a real end user system with infrastructure for Co-Inform scenarios and workflows to enable the components from WP3 and the policies and intervention strategies from WP2 to work together in order to address the requirements of WP1. Data processed in this WP will be mainly provided by work conducted in other WPs. However, when interface designs are released, feedback will be collected from consortium and stakeholders in collaboration with WP5.

The following datasets are being collected:

- **Knowledge base:** The information in the knowledge base is about the user and the environment and is the one used by the system itself to provide its features. The knowledge base is going to be implemented in cooperation with WP3. The format is still to be decided but it is safe to assume it will be some kind of database. The data in the knowledge base will be collected from different sources. It will be generated through the interaction the end user will have with the platform. The data will be updated during the use by participants. The knowledge base will be used by developers and technicians in the project for troubleshooting and debugging. Furthermore, it will be interesting for our social science researchers, especially during the evaluation (WP5).
- **User-related logs**: Information from user logs will be useful to monitor the user-system interaction. The logs are useful for behavior analysis as well, to improve usability and to determine whether the system is successful in its goals. Data collected from the logs will be used in WP5 for behavior analysis.

FAIR Data 2.1. Making data findable, including provisions for metadata

At this stage of the project metadata issues still remain open. Metadata-related information will be added during and at the end of the project in line with metadata conventions. All data files will be named so as to reflect clearly their point of origin in the Co-Inform project structure as well as their content. No further deviations from the intended FAIR principles are foreseen at this point.

2.2 Making data openly accessible

If it turns out that any of the datasets produced by the user-logs does contain personal information, then it will be treated in line with the project's guidelines.
We foresee no restrictions to the dataset, if and when completely anonymized.
No further deviations from the intended FAIR principles are foreseen at this point.

2.3. Making data interoperable

User logs: These can follow established formats for logging that are widely used and known by developers and technicians.

Knowledge base: Almost all possible options of technologies to be used in the knowledge base follow a well-known format or query language (i.e. MySQL).
No further deviations from the intended FAIR principles are foreseen at this point.

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

No further deviations from the intended FAIR principles are foreseen at this point.

3. Allocation of resources

The work to be done in making the data FAIR will be covered by the ordinary working budget for producing the deliverables.

4. Data security

No further deviations from the intended FAIR principles are foreseen at this point.

5. Ethical aspects

No further deviations from the intended FAIR principles are foreseen at this point.

6. Other

No other procedures are required to be put in place for project management data.

6.5 Data for WP5 Assessment of effect on misinformation-related practices and policies

1. Data Summary

The purpose of Data Collection in this WP is to gather information on the use of the misinformation platform in order to assess and evaluate it. Data will be collected during workshops and surveys with the users and behavior analysis will be conducted after users provide their feedback.

The following datasets are being collected:

- Notes and minutes of brainstorms and workshops (.doc format)
- Recordings and notes from interviews with stakeholders (.mps, .doc format)
- Transcribed notes/recordings or otherwise ‘cleaned up’ or categorized data. (.doc, .xls format). The files are initially stored as word and excel files. If it is possible to anonymize them and can be used for open access, these files will be stored in the equivalent Open Office format or as pdf.
- User-related logs: Information from user logs will be useful to monitor the user-system interaction. Data collected from the logs will be used for behavior analysis.

No data is being re-used. The data will be collected/generated by Co-Inform Consortium researchers before during, or after project meetings and through interviews with stakeholders. The data will be collected/generated by CUT and partners through interviews or surveys with stakeholders. All data gathering will take place within the EU.

FAIR Data 2.1. Making data findable, including provisions for metadata

At this stage of the project metadata issues still remain open. Metadata-related information will be added during and at the end of the project in line with metadata conventions. All data files will be named so as to reflect clearly their point of origin in the Co-Inform project structure as well as their content. No further deviations from the intended FAIR principles are foreseen at this point.

2.2 Making data openly accessible

The data will be stored in a trusted repository with an Open Access license. At the moment, there is no intention for patenting the information. By posting the data in an open repository with the Data Seal of Approval, we will ensure that the data will be made available for re-use. Only the final data set will be submitted in the repository. No further deviations from the intended FAIR principles are foreseen at this point. If it turns out that any of the datasets produced by the user-logs does contain personal information, then it will be treated in line with the project's guidelines. We foresee no restrictions to the dataset, if and when completely anonymized. No further deviations from the intended FAIR principles are foreseen at this point.

2.3. Making data interoperable

By storing the data in Open Office format, these data files can be read by commercial administrative tools, like Microsoft Office as well. In case MP3 files will be recorded, these are universal and can be played through multiple software tools. The collected data will be ordered so as to make clear the relationship between questions being asked and answers being given. It will also be clear to which category the different respondents belong (consortium members, external stakeholder). The data will use common social science data collection practice. One potential deviation in terms of privacy has to do with whether the answers will contain personal information. No further deviations from the intended FAIR principles are foreseen at this point.

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

The data will be stored in a trusted repository with an Open Access license. At the moment, there is no intention for patenting the information. By posting the data in an open repository with the Data Seal of Approval, we will ensure that the data will be made available for re-use. Only the final data set will be submitted in the repository. No further deviations from the intended FAIR principles are foreseen at this point.

3. Allocation of resources

The work to be done in making the data FAIR will be covered by the ordinary working budget for producing the deliverables.

4. Data security

Workshop and interview data will be gathered in the form of notes and audio recordings. Audio recordings and handwritten notes will be stored under lock in the offices of the Department of Computer and Systems Science (DSV) of Stockholm University in a physical storage space separate from the participant lists of workshops and interviewees.

Audio recordings and handwritten notes will be destroyed once they have been added to the typed notes from the workshops or interviews. In cases where audio recordings or handwritten notes are never added to the typed notes, they will be destroyed in any case no later than the end of the Co-Inform project. Typed notes (i.e. files in word or excel format) will be stored on encrypted disk drives on servers at the Department of Computer and Systems Science (DSV) of Stockholm University. Access will be granted in line with the project's procedures.

5. Ethical aspects

All workshop participants and interviewees will be asked to sign a consent form giving consent to use of the data in the Co-Inform project analyses and for the sharing of the data with others through FAIR measures. Consent for the two different uses will be specific. Consenting to the use of collected data for the purposes of the Co-Inform project analyses will be a mandatory requirement for workshop participation and the conduct of interviews. In cases of non-consent to FAIR use of the data, the statements produced by the person in question will be marked with a non-personal marker and eliminated from the dataset before publication.

If and when during data collection, there is any possibility of identifying individuals through their responses, the specific data will be treated as personal data and will be stored in line with the project's guidelines

6. Other

No other procedures are required to be put in place for project management data.

6.6 Data for WP6 Dissemination, Exploitation, and Communication

1.Data Summary

Two distinct types of Data collection will take place in the Dissemination WP. Data used in publications and academic journals and data used in the preparation and administration of the dissemination process (newsletter, event attendees' lists, invitations).

1. **Publications** in journals and on conferences describing project results. These publications will be published through green or gold open access publishing as much as possible. These will be available in pdf format. All partners will be responsible for disseminating the research data through papers. These results will be useful for researchers in the same or adjoining fields.

2. **Other communication items**: websites, press releases, interviews and other dissemination items will be made to create awareness of the project and to create a community of interested participants. All this information will be made available at least through our own website. The website will be continued for at least 2 years after the project has finished. At the moment we do not know the size of the dataset, since it will depend on the content that will be posted on there. Different target groups will be reached through several media as described in the

communication plan (D6.1). A newsletter will be used. The website will make use of Google Analytics, in order to further improve the use of the website. Google Analytics completely anonymizes the data of the visitors of the website and stores this information their own servers.

FAIR Data 2.1. Making data findable, including provisions for metadata

Data related to communication, dissemination and pre-marketing will be findable utilizing digital communications best practices, e.g. hashtag, metadata, keywords.

2.2 Making data openly accessible

Dissemination-related will be made public since it will not contain any sensitive material and its purpose is to make it public.

2.3. Making data interoperable

Not applicable.

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

Data related to communication, dissemination and pre-marketing will be allowed for reuse, following standard digital practices (mention the source). In addition, photos from the consortium will be released under Creative Commons licenses.

3. Allocation of resources

The work to be done in making the data FAIR will be covered by the ordinary working budget for producing the deliverables.

4. Data security

Information posted on the website will be posted through WordPress. Backups of the website will be provided and stored on servers at the Department of Computer and Systems Science (DSV) of Stockholm University. Non-sensitive data is stored on a Basecamp project management software accessible only by partners. Sensitive data, in terms of personal data and privacy is stored on secure servers in line with the project's guidelines. Privacy statements are provided on the website and the newsletter.
The newsletter is sent through Mailchimp. All registered users can opt out of the newsletter at any time in accordance with GDPR.

5. Ethical aspects

All participants in the consortium have agreed with posting their pictures online for dissemination items and project updates.

6. Other

No other procedures are required to be put in place for project management data.

6.7 Data for WP7 Management

1.Data Summary

Data Collected in this WP is related to information gathered for project management purposes. As these are record-keeping notes among consortium partners all participants will have provided their consent. This data will not be shared outside the consortium unless otherwise decided by all participants (unanimously) and consent provided.

The following datasets are being collected:

- Notes and minutes of brainstorms and consortium discussions (.doc format)
- Audio and video recordings and from consortium discussions (.mps, .doc format)

FAIR Data 2.1. Making data findable, including provisions for metadata

Not applicable.

2.2 Making data openly accessible

Not applicable

2.3. Making data interoperable

Data among partners will be shared in formats such as .doc, excel sheets, mp3 and shared through Basecamp project management tool.

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

Not applicable.

3. Allocation of resources

Not applicable.

4. Data security

Consortium discussions data will be gathered in the form of notes and audio recordings. Audio recordings and handwritten notes will be stored under lock in the offices of the Department of Computer and Systems Science (DSV) of Stockholm University in a physical storage space separate from the participant lists of workshops and interviewees.

Typed notes (i.e. files in word or excel format) will be stored on encrypted disk drives on servers at the Department of Computer and Systems Science (DSV) of Stockholm University. Access will be granted in line with the project’s procedures.

5. Ethical aspects

All participants in the consortium have agreed with posting their pictures online for dissemination items and project updates.
6. Other
No other procedures are required to be put in place for project management data.

ANNEX 1

Informed Consent for Co-Inform

1. Introduction

You are being invited to take part in the research project Co-Inform which aim is to create tools that will increase society's resilience to online misinformation and to generate more informed behaviors and policies. This document gives you information about the project and what it means to participate in it. At the end of the document you are asked for your consent to participate in the project including the personal data processing that will take place.

2. Purpose of the project

Misinformation is one of the most pressing issues that the online world is facing today. Digital technology has advanced at lightning speed, and algorithms used by social media platforms have been becoming more and more complex. Because of this, the consequences of online misinformation and its impact on real life are only now emerging. The ubiquitous and loose term “fake news” has risen to the surface and has become a hot topic frequently discussed in the public sphere.

A multitude of academic research has been conducted in recent years on the reasons online misinformation has spread so much, on its impact on society and on potential ways to effectively fight it. The Co-Inform research project aims to contribute towards this ambitious goal by focusing on intra-European, multidisciplinary research targeting three main stakeholder groups that could help turn this problem around: policymakers, journalists and citizens.

Academic surveys have shown that online misinformation is becoming more difficult to discern by the human eye. After asking readers to distinguish between a hoax and true articles, Stanford University researchers showed that humans made a correct identification just 66 percent of the times. And this research included both media-savvy and less educated readers. What does this show us? That online misinformation has the potential to deceive even readers with strong literacy skills. And due to the amplifying factor of social-media platforms, it can reach larger numbers than ever. Echo-chambers which are digital spaces where like-minded opinions just confirm each other, get boosted by algorithms and thus erect even thicker walls between online users with opposing views. Online misinformation can even lead to real-life consequences as recent anti-immigrant violence showed in Chemnitz, Germany. If we take it a step further and try to see the bigger picture, misinformation has the potential to lead to erosion of the public's trust towards institutions and media and to dangerously disrupt the political debate in Europe ahead of several crucial elections in 2019.

The Co-Inform project will aim at making an impact on the European society by conducting research in 3 different EU countries greatly affected by the combination of anti-immigration rhetoric and online misinformation. Co-Inform consortium partners believe that researching both the technological and behavioural aspects of this phenomenon is imperative in order to have a real impact on society. Online misinformation detection techniques that make use of big data analysis need to be combined with behavioural research regarding a user's attitude when confronted with false information. Co-Inform aims to make a difference by involving three categories of stakeholders that have the largest stake in the fight against misinformation: policymakers, journalists and citizens.

- **Citizens:** Using the methodology of co-creation, Co-Inform researchers will use a bottom-up approach to understand the end-users' needs when it comes to tools automatically detecting misinformation online. Co-Inform will use this feedback and researchers will be able to adjust and correct the tools' technological capabilities accordingly.
- **Policymakers:** Co-Inform will support policymakers with the creation of informed policies against the spread of misinformation. Support from a diverse group of International Institutions and NGOs will assist the Co-Inform consortium in widening the range of its research and reach of its results.
- **Journalists:** Co-Inform aims at providing our fact-checking partners with the adequate technology to overcome issues related to the high volume of online misinformation that they need to check. Furthermore, the effectiveness of current fact-checking methods will be assessed by examining public perception during all co-creation sessions.

The Co-Inform project aims at addressing these issues at a crucial moment in the European Union's history. Fighting online misinformation is more than getting rid of online trolls. It is about restoring trust towards public institutions and journalism and by extension restoring citizens' faith in the democratic process.

Co-Inform aims to engage all stakeholders in fighting misinformation by providing them with tools to identify misinformation online, understand how they spread and obtain verified information. The objective is to create tools that will increase society's resilience to online misinformation and to generate more informed behaviours and policies. The result of the project will also be published in scientific journals, workshops, conferences and on the website of the project.

The research project is conducted by a European research consortium which consist of nine (9) countries and is funded by the EU's Horizon 2020 program. More information about the project can be found on the website of the project: **www.coinform.eu**

3. Description of the study procedues

The part of the research project that you are invited to participate in will be conducted by Stockholm University and consists of a series of co-creation workshops with a group of 15-30 people who represents the three stakeholder groups of the project: citizens, journalists and policy makers. The aim of the co-creation workshops is to jointly discuss the needs and ideas for new methods, policies and digital tools for detecting and handling misinformation online. The workshops will be led by a workshop leader and be followed up by interviews and questionnaires. The workshops will start in December 2018 and last to November 2020.

4. Potential risks or discomforts of being in this study

There are no reasonable foreseeable or expected risks in the project, except if the outcome of the project would result in negative publicity, which could potentially cause discomfort for you as one of the participants in the project. This risk is, however, minimal, since you and the others participants' identity will be disclosed in the presentation of the project.

5. Confidentiality and use of the information

The voluntarily provided information will be used for research purposes only. The records of this study will be kept confidential in accordance to national applicable law. Research records will be kept in a locked file, and all electronic information will be coded and secured using a password protected file. The information that we will obtain, and store is audio and video, video and written documentation of the results of the workshops, interviews and questionnaires. We will also store certain personal data about you such as your name, address, contact details, age and occupation. The personal information will not be shared outside the research team beyond national legislation and will not be used in a manner which would allow identification of your individual responses in the workshops, interviews and questionnaires. Only summaries of the overall results from the workshops, interviews and questionnaires that you will participate in will be stored. The results of interviews and questionnaires will be anonymized prior to processing and publication, which means that individuals will not be able to be identified from the outcomes. Personal data will be retained in a protected file, separated from the outcomes of the participants' anonymous answers and discussions in interviews, questionnaires and workshops. Only summaries of workshops. interviews and questionnaires will be published in scientific journals and other publications. Personal information such as signed consent forms, names or email addresses will be destroyed within ten years of the initiation of the project. Responsible for your personal information is Stockholm University.

6. How do I get information about the results of the study?

According to the General Data Protection Regulation (EU) 2016/679 (GDPR) you have several rights. Of particular importance are rights (sometimes conditional) to be informed and have access to data, rectification and erasure, restrictions of processing, rights to data portability, right to object and request a portable copy of the personal data about you in a common format, and if you find necessary. If request that the information about you will be deleted. In order to do so, please contact the research leader of the project (see below contact information) or the Data Manager of the project at (email of the appointed Data Manager). If you are dissatisfied with the processing of your personal data, you are entitled to file a complaint with the Swedish Data Protection Authority (DPA), which is the national supervisory authority in Sweden.

7. Participation is voluntary

Your participation is voluntary, and you will not receive any compensation for your participation in the project. You are free to discontinue your participation in the project and withdraw your consent for the processing of your personal information at any time without any negative consequences. If you want to discontinue your participation, withdraw your consent, or if you have questions, concerns or complaints, please contact the primary investigator (see below contact information). You do not need to motivate your decision to discontinue your participation or withdraw your consent.

8. Contact information of the project

Primary investigator:

Phone:

Email

Visiting Address:

Postal Address:

9. Consent to participate in the project

☐ I have read and understood the project information dated **[**DD/MM/YYYY**]**, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.

☐ I consent voluntarily to be a participant in this project a**nd understand that I can refuse** to answer questions and I can withdraw from the project at any time, without having to give a reason.

☐ I consent that information about me is treated as des**cribed in the above information** about the project.

☐ I understand that participating in the project involves notes from the workshops, interviews and questionnaires.

☐ I am over 18 years old.

Signature

Place and Date

Name of participant **Signature**