CO-CHANGE
CO-create CHANGE in Research Funding and Performing

D7.1 Data Management Plan

Version 1.0

Submission date: July 2020
Dissemination Level: Confidential
Author(s): Peter Biegelbauer, Nikolas Reschen
Peer-reviewed by: Emad Yaghmaei

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873112

Project[1] Number: [873112]
Project Acronym: [Co-Change]
Project title: [Co-Create Change in Research Funding and Performing Organisations]

DATA MANAGEMENT PLAN

Document History

Name	Date	Version	Description
Nikolas Reschen	**29.06.2020**	**1.0**	**First draft up for peer review**
Nikolas Reschen	**31.07.2020**	**1.0**	**Revision after peer review through TU Delft and internal discussion at AIT**

Disclaimer: Note that this document is treated as a living document. Some specifications provided still need approval by the Project Management Committee (PMC) or the whole Consortium. A timetable on next steps has been provided in Table 1. Any changes to the Data Management Plan will be communicated as they occur and introduced in the next iteration of the document.

[1] The term 'project' used in this template equates to an 'action' in certain other Horizon 2020 documentation

Co-funded by the Horizon 2020 programme of the European Union

1. Data Summary

In the course of the Co-Change project, data will be collected from external sources as well as generated internally within the consortium. Internally generated data may include emails, minutes of meetings, and other communications among consortium members as well as indicators derived from external data and results from surveys, workshops or the like.

In the Co-Change project, most data are internally generated and will serve only administrative functions, nevertheless, some will be used directly as empirical evidence in research activities, for example in the context of the work with Change Labs (WP3). During the project the majority of the data collected and processed, apart from the ones serving administrative functions, will consist of externally sourced data with scientists, stakeholders and lab contact persons actively involved in the creation. To achieve the goals and objectives of the project external data need to be collected, processed and the results exchanged between the research partners to ensure learning and better understanding of Responsible Research & Innovation. In general terms, three phases of external data collection can be distinguished in the Co-Change project, as described in the following.

As a first step, Work Package 1 includes a stocktaking as well as institutional environmental and ecosystem analysis report. Most of these data are deriving from primary and secondary as well as additional interviews as outlined in the Work Package description in the proposal.

The second step in Co-Change is to interact with the Co-Change Labs. The data generated through this process are mainly deriving from interviews, but also from literature on the labs. This stage of data collection is the responsibility of WP 3. Findings from WP3 will also be used in the creation of deliverables of WP4 “Tool and Field Book for Implementing RRI Related Institutional Changes” and communicated in WP5 “Dissemination”. Regarding ethical aspects involved in generating data such as the collection data, see the ethics documents 8.1 – 8.3.

Third, data will be generated in WP 6 on “Monitoring and Assessment”. The data thus generated will be of more quantitative nature and therefore more suitable for further research within subsequent projects.

According to the information risk classifications of the project coordinator, all data generated within Co-Change will be of low or moderate risk. High risk data refers to strictly confidential information (e.g. patient records, passwords, and credit card numbers) or high-risk research (e.g. biomedical research, high risk chemical experiments) which is not the case within Co-Change.

More detailed information on data collection and utility in Co-Change can be found in Table 2 in the Annex.

What is the purpose of the data collection/generation and its relation to the objectives of the project?

In Co-Change data will be only collected in order to achieve the following objectives:

1. Describing the Co-Change Labs mainly in a qualitative way;
2. Getting data in order to test and validate the findings of the Co-Change Labs;
3. Build up knowledge based on the experiences made in the Co-Change Labs in the respective organisation;
4. Initiation of change towards RRI by workshop discussion with stakeholders and members of the community of practice.
5. Collection of data for dissemination of results
6. Creation and collection of data for Monitoring and Assessment

For data analysis and evaluation, the personal data is going to be dealt with in an anonymised or pseudonymised way so that it cannot be traced back to an identifiable natural person, but may retain criteria relevant for the analyses such as gender, age, job experience, cultural background etc.

As part of the creation of the “Co-change platform for co-creation and mutual learning”, data has to be stored and processed to ensure a well-functioning means of interaction. For a detailed overview of the data, information by work package will be provided in Table 2. To ensure compliance to data protection legislation, personal data:

- will only be used for the purpose of conducting the project, to the exclusion of other applications, in particular for commercial purposes;
- will not be disclosed, distributed, transferred or licensed to a third party, for any purpose whatsoever, without prior written authorisation from the supplier and in accordance with the authorisation/declaration necessary for the transfer;
- will be used and stored in accordance with the applicable legal and regulatory provisions. In particular, the recipient ensures that it has obtained any necessary authorisations and/or opinions and taken appropriate measures for the storage and use of the concerned Personal Data;
- will be returned to the supplier (or destroyed, at the supplier’s discretion and without any copy being made thereof) in the event of the withdrawal of the consent or the exercise of the opposition right of the person which would be communicated by the Supplier to the Recipient;
- will be stored exclusively on the premises of the recipient within the performance of the project and only used by scientists working on the premises of the Recipient or under its direct responsibility and with the same degree of security that applies to its own Personal Data.

What types and formats of data will the project generate/collect?

As stated above, for data analysis and evaluation the personal data is going to be dealt with in an anonymised or pseudonymised way so that it cannot be traced back to an identifiable natural person, but may retain criteria relevant for the analyses such as gender, age, job experience, cultural background etc. The pseudonymisation will be conducted through a coded reference (“key”) which will be stored separately.

Data formats collected in the different work packages can also be found in Table 2. In addition to these data, not all data types can be foreseen at this stage of the study. The Data Management Plan will thus be updated routinely on types of data collected.

Within the Co-Change project there will be no collection and processing of sensitive personal data that could reveal any political opinions, religious or philosophical attitudes/values nor any data concerning health or sex-life.

Data will primarily be of qualitative data describing the status quo, the ecosystem, the staff and the measures taken in Co-Change Labs. More details on the format will be communicated throughout the study.

Will you re-use any existing data and how?

Data collected through the stock-taking exercise of WP1 will be used as a basis of the study. Any re-used data will be clearly cited and acknowledged. Furthermore, data provided through participants (e.g. Co-Change Labs) and publicly available data will also be used for analyses. Public documents will be shared on the website of the project and, if desired, published by the European Commission. Confidential material will only be shared with the explicit consent of the European Commission.

A more detailed overview of data to be collected and data analyses to be conducted in all work packages (e.g. in the labs) can be found in Table 2. Raw and analysed data can be requested at the project coordinator. The release of those data will be closely coordinated with the European Commission and data subjects.

What is the origin of the data?

Data will be acquired through interviews, questionnaires, primary and secondary literature as well as observation. A detailed recruitment plan is provided below and is provided in more detail in Deliverable 8.1 on the “Recruitment of Humans”:

Recruitment plan

Target group
The recruitment of persons being involved in interviews, questionnaires and workshops, including the future conference is aiming to address persons from research and innovation.

Procedure
All ethical issues regarding human participants will be addressed by providing consent forms and confirm understanding and participative agreement in all consortium countries, including Serbia. No minors and individuals unable to give consent will be included in the research. Project Information Sheets and GDPR compliant Informed Consent Forms will be used for each event when dealing with human participants. All project partners will be involved in the recruitment process, so that a representative European perspective for the project results can be guaranteed. The project partners are also aiming to address people beyond their usual organisational and established networks.

Criteria and ethical issues
Recruits will be selected through staff of the partner organisations and their network via personal invitations or through public advertisement on different social media platforms. The recruitment policy will consider the gender dimension so that the final number of participants in the different events includes a balanced number of males and females. In every case, and at any time, the researchers of the project will ensure that participants fully comprehend that they have the right to discontinue involvement in the study at any time without explanation and without penalty.

Responses to questionnaires will be anonymised or pseudonymised during the processing, so that they cannot be traced back to named individuals, but may retain criteria relevant for the analyses such as gender, age, job experience, etc. As mentioned before the interview data will not be made accessible for processing without the informant`s consent.

What is the expected size of the data?

Given the mainly qualitative nature of data collection, the size of the data will likely be rather small. Quantitative data will mostly be collected for monitoring and assessment purposes.

In case more extensive quantitative analysis, increasing the expected size of data, the data management plan will be updated accordingly. More information on the exact nature and extent of data collection can be found in Table 2.

To whom might it be useful ('data utility')?

Data might be useful for researchers in the fields of Responsible Research & Innovation (RRI), Ethical, Legal and Social Aspects (ELSA) or other studies on ethical science. Data might also be of interest for organisations who are aiming to implement RRI methods in their research activities.

As data might also be of interest for third parties for malicious purposes, data security will be emphasised throughout the project.

2. FAIR data

Co-Change has chosen the Open Research Data pilot (ORDP) scheme under Horizon 2020. This requires Co-Change to create a DMP (the present document) and to follow the guidelines on FAIR data management, making research data “findable, accessible, interoperable, and re-usable” (FAIR) to the greatest possible extent, especially with regard to data needed to validate the results presented in scientific publications. If deviations from the FAIR principles occur, they should be explained in the DMP.[2]

[2] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

Personal data, meaning data including personal identifiers such as personal information of interviewed participants or survey respondents (and the ‘’keys’’ used for pseudonymisation), will not be made publicly available. This means that documents containing personal data will not be uploaded to the selected repository but will be kept in a safe way at the local repository of the partner(s) that collected the data.

2. 1. Making data findable, including provisions for metadata

It has to be ensured that the existence and some basic information about datasets collected and used can be easily discovered by other researchers to follow the first of the FAIR principles. This concept of findability is distinct from the concept of accessibility: A dataset might be findable but subject to access restrictions or it might be freely accessible but difficult to find.

In Co-Change, the major datasets will be made as findable as possible by the end of the project. How this will be achieved has to be put into concrete terms in the course of the project since the degree of details of data collected in the project still needs to be specified. Concrete information on data used can be found in Table 2. Any decisions about structure, labelling, storage, and provision of metadata will be made within the Project Management Committee and specified in future updates of the DMP.

Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers)?

The data will be labelled in a consistent and transparent manner in order to be used for further research. While ensuring the privacy of personal data, metadata analysis should be enabled through a clear data structure by the use of naming conventions.

At the current stage of progress, it is foreseen that Co-Change will obtain a DOI entry to make all public output of the project findable. The DOI is conceived as a generic framework for managing identification of content over digital networks, recognising the trend towards digital convergence and multimedia availability. The DOI system has been standardised through the International Standards Organisation, ISO (within the responsibility of committee ISO TC46/SC9, Identification and documentation) as “ISO 26324, Digital Object Identifier System”.

What naming conventions do you follow?

Deliverables will be named in the following format “DX.X_DATE_Name of Deliverable_V.X.DATAFORMAT” (e.g. D7.1_200629_Data Management Plan_V1.0.pdf). Individual data will be pseudonymised and assigned with numbers. Data entries will be machine-readable as far as possible. Potential changes to naming conventions will be discussed openly in future iterations and added to the Data Management Plan.

Will search keywords be provided that optimize possibilities for re-use?

Keywords will be used on platforms on which data created through the Co-Change project will be saved to facilitate the search for future research on the topic.

The following non-exhaustive list includes typical keywords to be used for Co-Change documents: *responsible; research; innovation; science; policy; RRI; Responsible Research and Innovation; RRI Tools; R&D management; Social innovation; Sustainable innovation; Corporate social responsibility; CSR; Industry; Business ethics; Research ethics; ELSA; Ethical, Legal and Social Aspects.*

This list of key words will be updated continuously throughout the project.

Do you provide clear version numbers?

Yes, clear version numbers and dates of release will be provided throughout the project. The system of numbering will be clearly discussed in the course of the project.

What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

Metadata created throughout the project are described in Table 2. This table as well as the data management plan will be updated according to new additions in terms of metadata. Metadata creation will also be discussed in the Project Management Committee.

2.2. Making data openly accessible

The second FAIR principle is to provide open access to the data used in a research project, enabling other researchers to verify the published findings of the project and conduct further research using the same data.
Co-Change aims to make all research data, with a few exceptions, used in the project openly accessible. The exact extent of shared deliverables, data and other products of the project as well as the exceptions will be discussed in the next upcoming consortium meeting.

To ensure the commitment to open access Co-Change will use the following approach:

- Consortium members will have access to the data collected in Co-Change, as data used in the project will be shared internally in the consortium. For this, AIT is responsible and hosts a MS SharePoint to share data files within the consortium. Final approval of the use of the MS SharePoint will be gathered at the next PMC meeting.
- All Co-Change deliverables which are classified as “public” will be made freely available for download on the Co-Change website (**http://www.cochangeproject.eu/**) after their submission to and approval by the Commission. For the website and uploading of deliverables, the leaders of WP 5 take responsibility. After the end of the project Co-Change does not commit to keeping the website operational indefinitely; it is foreseen that all public output will be placed in a suitable open-access repository to ensure their long-term accessibility. The repository will be chosen at a later stage of the project and documented in the updated DMP with a strategy for long-term storage and accessibility of data and deliverables. At this stage the following repositories are discussed for storage of project generated results in order to

make data more visible and accessible to the scientific, academic and territorial:
    - The Co-Change website (with links to the Social Media groups);
    - Individual Partner websites and the social media groups they are part of;
    - The portals of the academic publishers where scientific publications will be accepted;
    - Other official sources such as OpenAIRE/Zenodo[3];
    - Other potential repositories will be explored and discussed in the framework of the project's sustainability group.
- As stated before, data used and collected by Co-Change will be made openly accessible by the end of the project, unless it concerns personal data. The major datasets are will be updated and discussed in Table 2. Data will be made accessible in common file formats that can be read using open-source software.
- All personal data (e.g. from surveys, workshops, or other activities) will be anonymised or pseudonymised to protect the privacy of participants (see the respective deliverable D8.3 for details on ethics in Co-Change, also submitted in July 2020). All data will be anonymised in such a way that the value of the data as a research and verification tool is preserved. In addition, if stakeholders or other data providers, including partners, request that data they provide will be kept confidential, this request will be strictly obeyed. Measures taken to anonymise or pseudonymise data and decisions made to restrict data access upon request of the data providers will be included in the updated DMP.
- Technically, datasets will be made available in common file formats such as Microsoft Excel or Word. No advanced or prohibitively expensive software will be required to access the data.

Results will be shared and made openly accessible via:

- Open Access journals: Data should be disseminated through the submission to leading Open Access (if possible) scientific journals with broad dissemination. The partners will disseminate the results as swiftly as possible, but only after all other partners have been informed about the intention to disseminate as well as the content of the dissemination and have been given a reasonable timeframe in which they can object to (elements of) the intended dissemination. The time frame defined by the CA is 30 calendar days before the publication. Each partner will ensure open access to all publications relating to its results, free of charge. At a minimum, each partner makes publications and datasets without personal identifiers available by archiving it

[3] https://zenodo.org/communities/openaire/

in Zenodo, at the time of submission of the publication ('green' model). Additionally, the publications and datasets might be archived in an institution-based repository. If access cannot be granted, each partner will ensure open access to all peer-reviewed scientific publications relating to its results, free of charge.

Which data produced and/or used in the project will be made openly available as the default? If certain datasets cannot be shared (or need to be shared under restrictions), explain why, clearly separating legal and contractual reasons from voluntary restrictions.

Deliverables indicated as public in the grant agreement will be shared with a wider audience. Deliverables classified as confidential will only be shared with the contractee, the European Commission. Personal data, collected as part of the project, will only be shared publicly if agreed with individuals included in the dataset.

Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if relevant provisions are made in the consortium agreement and are in line with the reasons for opting out.

How will the data be made accessible (e.g. by deposition in a repository)?

Deliverables indicated as public in the grant agreement will be made available through channels of the European Commission, where suitable, as well as on the Co-Change website. If deemed appropriate, data will be shared on the data repository Zenodo- The approval to use Zenodo will be gathered at the next PMC meeting.

Scientific publications might be developed based on data collected throughout the project. Specifications on the access rights for data during and after the project, general rules and specific rules for Co-Change can be found in Section 9 of the Consortium Agreement. As already stated, personal data will only be collected following ethical guidelines on data collection and anonymised in an appropriate manner. More information on this can be found in Deliverable 8.3.

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

The Software necessary to access the data will depend on the nature of the data. The Microsoft Office Suite (Word, Excel, PowerPoint) will be used as the main software to access and share data. Other software, such as STATA, R or SPSS, might be required for accessing additional data. The research team will aim to provide data formats that can be accessed with open source software.

Is documentation about the software needed to access the data included?

Documentation about recommended software for further analysis will be provided.

Is it possible to include the relevant software (e.g. in open source code)?

Links to download the appropriate software will be provided where appropriate. It is not planned to include the relevant software.

Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories which support open access where possible.

Data including more sensitive or confidential data will be saved on the AIT SharePoint. Metadata, documentation and code will be made available through Zenodo

Have you explored appropriate arrangements with the identified repository?

AIT has gathered extensive information on the use of secure storage opportunities for data on the AIT SharePoint and with data repositories such as Zenodo.

If there are restrictions on use, how will access be provided?

Access to data will be managed by the project coordinator. Data on SharePoint can only be accessed on invitation. Consortium partners will be instructed about the appropriate conduct with sensitive data.

Is there a need for a data access committee?

At this stage of the project, there is no need for a data access committee. In case this changes, the data management plan will be adjusted.

Are there well described conditions for access (i.e. a machine-readable license)?

For every dataset or document, clear descriptions of how to access and process the data will be given. Open source software to process or analyse data will be strictly preferred.

How will the identity of the person accessing the data be ascertained?

Access will only be granted to trustworthy and known mail addresses. E-mail addresses of consortium members have been gathered through secure communication at the beginning of the project.

2.3. Making data interoperable

To allow data exchange between researchers, institutions, organisations and countries and to make the data compatible with other, existing datasets or particular tools of analysis the third FAIR principle is followed to ensure that research data can be used by others without first undergoing costly and time-consuming adaptations.
Most of the output collected in Co-Change will be of a qualitative nature, consisting in summary reports, survey responses, interview transcripts, workshop minutes and similar products.

A list of collected data is shown in Table 2 in the Annex and will be updated according to ongoing developments of the project. Reporting documents and datasets will be stored and made available in common file formats, such as pdf or CSV, that can be read using open-source software. Technological interoperability is not considered a major concern by the consortium. Also, it is not deemed necessary or worthwhile to encode data using a database processing language.

The consortium is aware that the value of the datasets that will be created within the project depends on the ease with which the data can be compared to other, similar datasets. Therefore, the consortium will take care of this issue through careful metadata provision and align as much as possible with terminologies and methods commonly used in research fields relevant for Co-Change, namely Responsible Research and Innovation as well as associated research fields.

Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?

If deemed appropriate, data will be shared in an interoperable format to be used for further research. Data anonymisation and pseudonymisation standards apply. To pseudonymise data, each participant needs to be given a numerical code to replace identifying information and ensure anonymity. The document containing the personal identifiers and numerical codes (the 'key') needs to be stored separately from the document containing the anonymized data.

What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?

The applied data and metadata vocabularies, standards and methodologies to enable interoperation of data will be decided in the course on the study. The Data Management Plan will be updated accordingly.

Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability?

As discussed above, the use of standard vocabulary will be decided in the course of study. The Data Management Plan will be updated accordingly.

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?

It is planned to use standard vocabulary and ontology. In case uncommon or project specific ontologies are necessary, mappings will be provided.

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

The Project Management Consortium will take measures to make it possible for third parties to access, mine, exploit, reproduce and disseminate data. If such access cannot be granted, each partner will aim to ensure open access to all peer-reviewed scientific publications relating to its results, free of charge. Data access might not be granted to third parties when this would interfere with relevant data protection legislations in the countries participating in this project and any applicable EU legislation regarding data protection.

Consortium partners will decide if a license (e.g. CC BY, CC BY-SA) needs to be put to the dataset before publication. Data-access will be preserved and maintained for a minimum of 10 years after the project has finished and after the moment of publication.

How will the data be licensed to permit the widest re-use possible?

It is aimed to make public data broadly available. Consortium partners will decide if a license (e.g. CC BY, CC BY-SA) needs to be put to the dataset before publication.

When will the data be made available for re-use? If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Data suitable for release publicly will be made available after confirmation of the European Commission, the potentially necessary anonymisation or pseudonymisation and, if necessary, the granted permission of the data subjects described in the data.

Are the data produced and/or used in the project useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why.

It is aimed to make data usable for third parties if classified as public data. Data release will be closely coordinated with the European Commission as well as data subjects described by the data. Any changes to the release policy will be updated in the Data Management Plan and communicated publicly, through e.g. the project website.

How long is it intended that the data remains re-usable?

Data-access will be preserved and maintained for a minimum of 10 years after the project has finished and after the moment of publication. In case this number changes, it will be indicated in the DMP.

Are data quality assurance processes described?

Qualitative data, produced through interviews, workshops, conferences etc. will be recorded through notes and minutes. Their accuracy will be checked by another person. All products and deliverables of the study are peer-reviewed internally by consortium partners. Quantitative data produced throughout the project will similarly be reviewed internally. Improvements and adjustments to the quality assurance processes will be reviewed throughout the project and added to the Data Management Plan.

Further to the FAIR principles, DMPs should also address:

3. Allocation of resources

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

The costs to make data fair have not been discussed yet in the consortium, but will be an agenda point for the next PMC meeting. Costs for one Open Access publication have been estimated around 2,500 € in the consortium agreement.

How will these be covered? Note that costs related to open access to research data are eligible as part of the Horizon 2020 grant (if compliant with the Grant Agreement conditions).

The costs for Open Access publications have been covered in the budget in “Other Goods and Services”. The estimation of other costs to make data FAIR will be subject of discussion in the upcoming PMC.

Who will be responsible for data management in your project?

The Project Management Consortium (PMC) as well as the coordinator will be responsible for the general data management in the project. For work package specific data collection not generally shared among consortium members, work package leaders will be responsible with the management of those data. The management of created datasets will be subject of discussion of the next PMC.

General data management including the necessary updates of the DMP is centred in WP7, led by AIT. The need for resources for making Co-Change's research data FAIR is difficult to estimate at this stage as it depends partly on decisions that have not yet been made, such as the choice of long-term depository for the datasets, and on levels of required effort that cannot be reliably determined until the data have been collected. Preferred options for making data publicly available are the cooperation with other EU funded projects offering services for free usage or open access repositories of the project partner organisations or the storage on open access repositories of a project partner. Zenodo, the preferred option, is funded by the EU, which means archiving data in this repository will be free of charge.

Within the project several publications in the form of papers based on Co-Change data in academic journals are planned by consortium members. These papers will be published on an open-access basis, following the general H2020 regulations. The costs for open access publications are regarded as an expense eligible for reimbursement under the Grant Agreement during the duration of the project. Costs for open access publications after the end of the project will fall within the author's own budget.

Are the resources for long term preservation discussed (costs and potential value, who decides and how what data will be kept and for how long)?

As discussed above, estimations are difficult to assess at this stage, but will be clarified in the next consortium meeting and added to the Data Management Plan.

4. Data security

What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?

Transfer of the personal data between the EU and non-EU countries is strictly limited to project partners.

This research follows the guidelines based upon Article 89 General Data Protection Regulation and Regulation (EU) 1291/2013 on establishing Horizon2020, as well as the protection of the natural persons in relation to the processing of personal data according to regulation EU 2016/675. The consortium also includes the University of Novi Sad in Serbia. A detailed discussion on the safe storage and transfer of sensitive data from and to third countries will be discussed in the next PMC. However, until equivalence of data protection can be assured, participants in the study will be informed that a European Union level of data protection cannot be guaranteed, as there might not be an equivalent data protection agency or the same level of rights for individuals described in datasets. The Serbian legal situation is described in more detail below.

A document informing all consortium members of the legal situation and the correct conduct will be prepared. The matter will also be discussed in the next consortium meeting and information forms, signed by all consortium partners, will be collected.

In case activities undertaken in non-EU countries raise ethics issues, the applicants must ensure that the research conducted outside the EU is legal in at least one EU Member State. In fact, on November 9, 2018, Serbia's National Assembly enacted a new data protection law.

The Personal Data Protection Law, which became effective on August 21, 2019, is modelled after the EU General Data Protection Regulation ("GDPR"). Key features of the new Serbian law include:

Scope - the Personal Data Protection Law applies not only to data controllers and processors in Serbia but also those outside of Serbia who process the personal data of Serbian citizens.

Database registration - the Personal Data Protection Law eliminates the previous requirement for data controllers to register personal databases with the Serbian data protection authority ("DPA"), though they will be required to appoint a data protection officer ("DPO") to communicate with the DPA on data protection issues.

Data subject rights - the new law expands the rights of data subjects to access their personal data, gives subjects the right of data portability, and imposes additional burdens on data controllers when a data subject requests the deletion of their personal data.

Consent - the Personal Data Protection Law introduces new forms of valid consent for data processing (including oral and electronic) and clarifies that the consent must be unambiguous and informed. The prior Serbian data protection law only recognized handwritten consents as valid.

Data security - the new law requires data controllers to implement and maintain safeguards designed to ensure the security of personal data.

Privacy by Design - the new law obligates data controllers to implement privacy by design when developing new products and services and to conduct data protection impact assessments for certain types of data processing.

Data transfers - the Personal Data Protection Law expands the ways in which personal data may be legally transferred from Serbia. Previously, data controllers were required to obtain the approval of the Serbian DPA for any transfers of personal data to non-EU countries. The new law permits personal data transfers based on standard contractual clauses and binding corporate rules approved by the Serbian DPA. Organizations can also transfer personal data to countries deemed to provide an adequate level of data protection by the EU or the Serbian DPA or when the data subject consents to the transfer.

Data breaches - like the GDPR, the new law requires data controllers to notify the Serbian DPA within 72 hours of a data breach and will require them to notify individuals if the data breach is likely to result in a high risk to the rights and freedoms of individuals. Data processors must also notify the relevant data controllers in the event of a data breach.

Is the data safely stored in certified repositories for long term preservation and curation?

Project deliverables as well as data will be stored for long term preservation in an appropriate measure. Possible storage options have been screened (an overview can be found in below). Final approval to use the AIT SharePoint will be gathered at the next consortium meeting.

Storage: File sharing platform AIT SharePoint

To store and share data with other partners, partners of Co-Change make use of file sharing platform SharePoint. The Co-Change main page as well as the sub-pages are accessible for all consortium partners. Specific pages are only accessible for a selection of relevant (consortium) partners.

All data on the AIT SharePoint is encrypted at datacentre level to secure data storage. However, this does not mean that documents uploaded to the AIT SharePoint are automatically encrypted. Therefore, researchers should not leave their computer unprotected. This means, researchers should not only sign out from AIT SharePoint before leaving the room, they should also close their browser.
Persons who stop being involved in the project will be denied access to data and results on AIT SharePoint and any other repository as soon as notice has been given to the Coordinator.

Storage: Institutions internal network system and the potential need for encryption

Documents containing personal data – referring to personal identifiers – need to be stored at institutions internal network system in a secured way. Depending on the security level of institutions' internal network systems, these documents need to be encrypted. This can be done by special software. Word and Excel files can be encrypted using a password. Although documents are encrypted, researchers may not leave computers unprotected. Computers should always be locked with a password before leaving the room.

Storage: Employees

Consortium members should comply with the local legislation of their country regarding the removal of personal data after all data has been generated.
Partners need to make sure their employees take necessary measures to prevent unauthorized access to files which include personal data. These may include, among others, the following:
o The storage of personal data on private notebooks, mobile devices or external hard disks should be prevented.
o Transcripts or voice recordings held outside of the approved systems of the partner must be stored on an encrypted device for temporary storage only. They must be transferred to the systems of the partner and deleted from temporary storage as soon as possible.
o Non-useful copies of data and results need to be destroyed after the project has finished.

Survey tools

When using a survey tool within Co-Change, or if free online survey tools are used, the Terms and Conditions should be read carefully. The Terms and Conditions should tell the researcher:

- Where the provider stores the data; this should be in Europe;
- If the data will be used for commercial activities.
- If the personal data of your respondents is well protected.

In doubt, the partners are encouraged to consult the Coordinator to check if the service provider they are dealing with is operating in line with the GDPR. In such cases, the coordinator will consult the legal experts of the coordinator's institution.

Archiving and preservation (long term)

Storage at AIT platform

According to the internal AIT quality management specifications, project data must be stored for 10 years after the end of the project. At the end of the project all data from the AIT SharePoint will be moved to AIT servers so that AIT can guarantee the availability and the restricted access to stored data for eligible persons. Besides the standard backup procedure, AIT has no further dedicated central data archiving system. Because of that, AIT cannot guarantee the unchangeability of stored data. Additional research data such as personal notes, unused photos and video clips etc. will be safely deleted and discarded after the end of the project. This includes all data not intended to be made publicly available for the long term.

Storage at Zenodo and partner's networks

After processing of data during the course of the project, relevant data will in principle be archived safely in repository Zenodo – and potentially in partners' own repositories – at the time of submission of publications ('green' model). Zenodo is an open and public research data repository funded by the European Commission (via the OpenAire Projects FP7 and Horizon 2020), CERN and the Alfred P. Sloan Foundation. Data containing personal identifiers, which includes, among others, transcripts, meeting notes and minutes, should not be archived on Zenodo, but should be archived in partners' own network with adequate level of security. Near the end of the project and before archiving a detailed overview will be created to confirm which data will be archived in Zenodo and which data will be archived in partners' own networks only.
It is recommended to archive text documents in PDF/A format (rather than in MS Word), to guarantee access (in its original form) during the entire archiving period.

Data transfer and security

Research data and stakeholder data are treated differently in this project.
Stakeholder data, including personal identifiers, can be transferred among the consortium partners without restrictions. Certain personal identifiers of stakeholders (e.g. name, position and organisation) can be included in the external reports, depending on the consent they provided.
Research data is subject to a number of restrictions for transfer. In case of research data, it is only allowed to transfer pseudonymized data among partners of the consortium. This means, research data containing personal information – called personal identifiers – should be pseudonymized to secure personal information before

it is transferred to other partners. The AIT SharePoint can be used to transfer research data, including pseudonymized transcripts or survey results (meaning data without personal identifiers).
As described in the CA, pseudonymisation means: ‘’the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person’’.
To pseudonymise data, each participant needs to be given a numerical code to replace identifying information and ensure anonymity. The document containing the personal identifiers and numerical codes (the ‘key’) needs to be stored separately from the document containing the anonymized data.
When personal data that is collected for research purposes (i.e. that is also research data) needs to be transferred, this needs to be processed in accordance with the article 11.9 of the CA:
“Each Party ensures that any processing of personal data carried out for or in occasion of the Project is legitimate and compliant with both the General Data Protection Regulation (EU) 2016/679 and its respective national Data protection regulation. Each Party also ensures that any supply of personal data to any other Party is legitimate and compliant with both regulations. In case personal Data is processed for the implementation of the Project, a Personal Data Addendum (PDA) shall govern the processing and, use of Personal Data collected and processed during the actual performance of an activity. A PDA is not needed for the use of communications details of data subjects processed by the Parties for the purpose of administering this Project, including Names, Email addresses and other related tele contact information which shall only be processed to the limited extent required to manage the business relation between the Parties. The PDAs will be prepared, agreed and formalized before a separate activity by the Parties concerned.”

Strategy to transfer personal data, in the context of research data
To transfer the personal identifiers of research data (e.g. keys), the AIT SharePoint cannot be used, since the entire consortium has access to this platform. Therefore, a specific service should be used to transfer personal data. As of now, it is intended to use the tool FileSender. ***FileSender*** is an open source web-based application to send documents securely. This means it is specifically aimed to transfer sensitive data, including personal data. However, personal data should be encrypted before sending for extra security. The approval for the use of FileSender will be collected at the next PMC.

Data transfer agreements
In the context of research data, before the transfer of personal data to specific partner(s), a separate bilateral or multilateral data transfer agreement specifying the conditions of transfer and processing of personal data by the recipient should be agreed on by the supplier and the recipient data. If personal data needs to be transferred, a basic agreement will be developed by the coordinator, which can be used by the partners. Nevertheless, consortium partners should still comply to their countries’ local additional legislation regarding the privacy of personal data.
However, if data is collected as a collaborative effort between consortium partners, there is no need for a separate bilateral or multilateral data transfer agreement. For

security reasons during the transfer, pseudonymisation is still necessary and personal data (the keys) still needs to be sent separately and securely to the other consortium partner(s).

Data recovery
All consortium partners should use data storage facilities that allow for data recovery. Such data recovering strategies should be checked in advance.

MS Teams
To store and share stakeholder level, which is not containing sensitive or personal information, with other partners, partners of Co-Change will make use of the file sharing platform Microsoft Teams. All data this platform is encrypted at datacentre level to secure data storage. Partners and users of MS Teams are advised not to leave their computer unprotected or sign out and close the browsers should they leave the room. It is the responsibility of project partners to save administrative data on the project MS Teams page and to delete the data on their local saving devices. The project MS Teams is curated by AIT, who makes sure all measures are applied in order to safeguard the data form being accessed by third parties. Consortium members are advised not to save sensitive or personal data on MS Teams. Teams will also be used as a communication platform for video conferences.

Persons who stop being involved in the project will be denied access to data and results on the MS Teams platform and any other repository as soon as notice has been given to the Coordinator.

5. Ethical aspects

Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

The protection of personal data according to the Regulation EU 2016/679 is given high priority in the Co-Change project. Data will only be shared if they are anonymised or pseudonymised or do not include personal data, unless given explicit consent by the respective individuals included in the data set.

Is informed consent for data sharing and long-term preservation included in questionnaires dealing with personal data?

For questionnaires, workshop participations or subcontracts (e.g. for the Advisory or Sounding Board), consent and data sharing, informed consent is being ensured through a Data Processing Agreement as outlined in the GDPR. Participants are informed about the duration their data is being stored. The template will be attached to the Data Management Plan after approval of the European Commission.

6. Other issues

Do you make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones?

At this stage, no other procedures are applied. Any changes to this will be stated in the next iteration of the Data Management Plan.

7. Further support in developing your DMP

The Research Data Alliance provides a Metadata Standards Directory that can be searched for discipline-specific standards and associated tools.

In the course of the project, data management standards will be updated constantly according to ongoing changes in legal specifications in order to keep data management at the state-of-the-art. The Research Data Alliance's materials, the EUDAT B2SHARE tool as well as other sources will be consulted for constant improvements of data management standards.

The EUDAT B2SHARE tool includes a built-in license wizard that facilitates the selection of an adequate license for research data.

Useful listings of repositories include:

Registry of Research Data Repositories

Some repositories like Zenodo, an OpenAIRE and CERN collaboration), allow researchers to deposit both publications and data, while providing tools to link them.

At this stage of the study, the use of Zenodo, which allow the use of GitHub repositories, is planned. Zenodo is preferable, as it has been developed through the OpenAIRE Consortium through the Horizon 2020 programme and thus developed in cooperation with the European Commission.

Other useful tools include DMP online and platforms for making individual scientific observations available such as ScienceMatters

Table 1 includes an overview of actions to be addressed as a follow-up to the initial draft of the Data Management Plan.

Table 1: Action points as a follow-up to the first iteration of the Data Management Plan

Action	Date	Audience
Discussion and approval of the AIT SharePoint as the appropriate data repository and FileSender as Key-sharing platform	4 August 2020	PMC
Discussion on Work Package plan and necessary action in DMP	4 August 2020	PMC
Discussion on which deliverables as well as products (e.g. interviews) should be made publicly available	Consortium meeting on 25 September 2020	All Consortium partners

Action	Date	Audience
How long access rights will be provided to which party	4 August 2020	PMC
Discussion on cost, creation and standardisation of metadata and Open Access	4 August 2020	PMC
Discussion on run-time of website	4 August 2020	PMC esp. WP5 leaders
Discussion and clarification of the data security situation in Serbia	4 August 2020	PMC

SUMMARY TABLE 1

FAIR Data Management at a glance: issues to cover in your Horizon 2020 DMP

This table provides a summary of the Data Management Plan (DMP) issues to be addressed, as outlined above.

DMP component	Issues to be addressed
1. Data summary	• State the purpose of the data collection/generation Data will be collected for the purpose of the conduct of the study with the aim to study and implement RRI methods in research organisations. Data might also be collected to allow for further research in the future. • Explain the relation to the objectives of the project The different objectives of the work packages depend to some extent to the collection of data from the literature, qualitative data through stakeholder interaction as well as complementing quantitative data. • Specify the types and formats of data generated/collected The types and formats of the data will be collected and communicated in the next iteration of the data management plan. • Specify if existing data is being re-used (if any) Data collected through the stock-taking exercise of WP1 will be used as a basis of the study. Any re-used data will be clearly cited and acknowledged. Further re-use of data will be specified by work package in the next iteration of the data management plan. • Specify the origin of the data Data will be acquired through interviews, questionnaires, primary and secondary literature as well as observation Further data collection will be specified by work package in the next iteration of the data management plan. • State the expected size of the data (if known) Through the mainly qualitative nature of the data, large data collection is not expected, any changes to this will be mentioned in the data management plan. • Outline the data utility: to whom will it be useful Data might be useful for researchers in the fields of Responsible Research & Innovation (RRI), Ethical, Legal and Social Aspects (ELSA) or other studies on ethical science.
2. FAIR Data	• Outline the discoverability of data (metadata provision)

2.1. Making data findable, including provisions for metadata	Co-Change has chosen the Open Research Data pilot (ORDP) scheme under Horizon 2020. This requires Co-Change to create a DMP (the present document) and to follow the guidelines on FAIR data management, making research data "findable, accessible, interoperable, and re-usable" (FAIR) to the greatest possible extent, especially with regard to data needed to validate the results presented in scientific publications. • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? The data will be labelled in a consistent and transparent manner in order to be used for further research. While ensuring the privacy of personal data, metadata analysis should be enabled through a clear data structure by the use of naming conventions. DOIs will be entries will be applied. • Outline naming conventions used Deliverables will be named in the following format "DX.X_DATE_Name of Deliverable_V.X.DATAFORMAT" • Outline the approach towards search keyword Keywords will be used on platforms on which data created through the Co-Change project will be saved to facilitate the search for future research on the topic. Typical keywords can be found in the document. • Outline the approach for clear versioning Clear version numbers and dates of release will be provided throughout the project. The system of numbering will be clearly discussed in the course of the project. • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how Metadata created throughout the project are described in Table 2. This table as well as the data management plan will be updated according to new additions in terms of metadata.

2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so Data used and collected by Co-Change will be made openly accessible by the end of the project, unless it concerns personal data after having the approval of the European Commission and potentially the data subjects. The extent of data that will be shared is specified in Table 2. • Specify how the data will be made available Data will be made available through Zenodo. • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? The Software necessary to access the data will depend on the nature of the data. The Microsoft Office Suite (Word, Excel, PowerPoint) will be used as the main software to access and share data. Other software, such as STATA, R or SPSS, might be required for accessing additional data. The research team will aim to provide data formats that can be accessed with open source software. Documentation about recommended software for further analysis will be provided. Links to download the appropriate software will be provided where appropriate. It is not planned to include the relevant software. • Specify where the data and associated metadata, documentation and code are deposited Data including more sensitive or confidential data will be saved on the AIT SharePoint. Metadata, documentation and code will be made available through Zenodo • Specify how access will be provided in case there are any restrictions Access to data will be managed by the project coordinator. Data on SharePoint can only be accessed on invitation. Consortium partners will be instructed about the appropriate conduct with sensitive data.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. If deemed appropriate, data will be shared in an interoperable format to be used for further research. Data anonymisation and pseudonymisation standards apply. To pseudonymise data, each participant needs to be given a numerical code to replace identifying information and ensure anonymity. Standard data and metadata vocabularies will be used and communicated throughout the study. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies? The applied data and metadata vocabularies, standards and methodologies to enable interoperation of data will be decided in the course on the study. The Data Management Plan will be updated accordingly.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible It is aimed to make public data broadly available. Consortium partners will decide if a license (e.g. CC BY, CC BY-SA) needs to be put to the dataset before publication. • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed

	Data suitable for release publicly will be made available after confirmation of the European Commission, the potentially necessary anonymisation or pseudonymisation and, if necessary, the granted permission of the data subjects described in the data. • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why It is aimed to make data usable for third parties if classified as public data. Data release will be closely coordinated with the European Commission as well as data subjects described by the data. • Describe data quality assurance processes Qualitative data, produced through interviews, workshops, conferences etc. will be recorded through notes and minutes. Their accuracy will be checked by another person. All products and deliverables of the study are peer-reviewed internally by consortium partners. Quantitative data produced throughout the project will similarly be reviewed internally. • Specify the length of time for which the data will remain re-usable This will be determined throughout the study.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs The costs to make data fair have not been discussed yet in the consortium, but will be an agenda point for the next PMC meeting. Costs for one Open Access publication have been estimated around 2,500 € in the consortium agreement. • Clearly identify responsibilities for data management in your project The costs for Open Access publications have been covered in the budget in "Other Goods and Services". The estimation of other costs to make data FAIR will be subject of discussion in the upcoming PMC. • Describe costs and potential value of long term preservation As discussed above, estimations are difficult to assess at this stage, but will be clarified in the next consortium meeting and added to the Data Management Plan.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data Sensitive and Personal data will be stored on the AIT SharePoint. Safeguarding secure storage will be ensured through a number of measures. Data recovery will be assured through constant backups and an automatic version history.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former The protection of personal data according to the Regulation EU 2016/679 is given high priority in the Co-Change project. Data will only be shared if they are anonymised or pseudonymised or do not include personal data, unless given explicit consent by the respective individuals included in the data set.

6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any) Will be updated according to new developments.

Annex

Table 2: Data collection by work package

			What is the intention, the objective for collecting the data?	Which data is collected?	How do we collect the data?	What is the type of the data? What is the format of the data?	Which source do we use for the data? (re-using existing data or not)	What is the usefulness of the data?	How does the result look like? How can we recognise?
WP 1 Project Management									
D1.1	Stocktaking report	TECNALIA							
D1.2	Institutional environment and ecosystem analysis report	VTT							
WP 2 Co-Change Platform									
D2.1	Guidelines for forums and labs	AIT							
D2.2	Short Report on Forum 1	AIT							
D2.3	Short Report on Forum 2	AIT							

			What is the intention, the objective for collecting the data?	Which data is collected?	How do we collect the data?	What is the type of the data? What is the format of the data?	Which source do we use for the data? (re-using existing data or not)	What is the usefulness of the data?	How does the result look like? How can we recognise?
D2.4	Short Report on Forum 3	AIT							
D2.5	Short Report on Forum 4	AIT							
D2.6	Update to Co-Change Guidelines	VTT							
WP 3 Co-Change Labs									
D3.1	Situated adaption of guideline on common framework for change labs	VTT							
D3.2	Report on call for innovative RRI practices	TECNALIA							
D3.3	Report on change labs	TECNALIA							
D3.4	Report on sustainability plan for Co-Change labs	TECNALIA							
WP 4 Tools									
D4.1	Tool for a systemic	VTT							

			What is the intention, the objective for collecting the data?	Which data is collected?	How do we collect the data?	What is the type of the data? What is the format of the data?	Which source do we use for the data? (re-using existing data or not)	What is the usefulness of the data?	How does the result look like? How can we recognise?
	RRI self-evaluation and impact assessment								
D4.2	Toolbox on implementing RRI on organization and system levels	VTT							
WP 5 Dissemination									
D5.1	Communication and dissemination plan	ESSRG							
D5.2	Construction of website portal	ESSRG							
D5.3	Policy brief 1	ESSRG							
D5.4	Policy brief 2	ESSRG							
D5.5	Final report on dissemination activities	ESSRG							
WP 6 Monitoring and Assessment									
D6.1	Assessment of added value of RRI based on	TU Delft							

			What is the intention, the objective for collecting the data?	Which data is collected?	How do we collect the data?	What is the type of the data? What is the format of the data?	Which source do we use for the data? (re-using existing data or not)	What is the usefulness of the data?	How does the result look like? How can we recognise?
	change labs and KPIs								
D6.2	Comparative analysis of the change labs: Insights emerging from the application of the framework to the change labs	TU Delft							
WP 7 Project Management									
D7.1	Data management plan	D7.1	The document informs in great detail about the conduct of data collection, storage and distribution and the safeguards to ensure the safety of personal information	Data on the purpose of data collection in the different work packages is collected (in this table).	Consortium members will be asked to fill in the information for their respective deliverables.	Summary data on the purpose and extent of data collection will be provided. No particular format will be applied, as data collection will be very diverse across deliverables	Sources will be provided by the work package leaders.	Provide an overview of data collected in the work packages in order to adapt the data management plan and thereby facilitate the safe storage of data and distribution of potential FAIR data.	The data will be provided as is the case for this entry.
D7.3	Update management plan	D7.3							
7.3	H - POPD - Requirement No 4	AIT							
WP 8 Ethics requirements									

			What is the intention, the objective for collecting the data?	Which data is collected?	How do we collect the data?	What is the type of the data? What is the format of the data?	Which source do we use for the data? (re-using existing data or not)	What is the usefulness of the data?	How does the result look like? How can we recognise?
D8.1	H - Requirement No. 1	AIT	The document specifies which recruitment criteria is applied for humans	No data is collected in the deliverable. It describes the process for the collection in other deliverables though.	No data collected.	No data collected	No data collected	No data collected	No data collected
D8.2	H - POPD - Requirement No. 2	AIT	The document provides information on the informed consent procedure. It provides the potential participants of workshops and interviews about the purpose of the data collection for the respective task.	No data itself will be collected through this document. It rather informs about data collection. When issued for the separate tasks, the signature of the respective persons will be collected.	No data collected.	No data collected	No data collected	No data collected	No data collected
D8.3	POPD - Requirement No. 3	AIT	The document informs about the appointment of a Data Protection Officer, the security measures for data protection, the data transfer procedures and the ethical and legal framework of data collection and storage.	No data is collected, but information about the conduct with data is provided	No data collected.	No data collected	No data collected	No data collected	No data collected