COST Action CA16121

From Sharing to Caring:
Examining Socio-Technical Aspects of the Collaborative Economy

Handbook on Ethics, Authorship and Data Management

SharingandCaring.eu

Table of Contents

1. Research Data Gathering and Management Guidelines ……... .p. 4
1.1. Data Availability ……... .p. 4
1.2. Data Collection, Processing and Personal Data Protection ……... .. p. 5
1.2.1. Informed Consent ……..…… .p.5
1.2.2. Personal and Sensitive Data……/…..…… .p.5
1.2.3. Anonymity and Confidentiality…… .p.6
1.3. Data Storage, Security and Accessibility ……..……. p.6
1.*3.1. Security Measures…….. p.6*
1.3.2. Data Ownership and Data Access …….. p.7
1.3.3. Sharing and Caring Members Only Platform ……..……..p.8
1.3.4. Sharing and Caring Public Website ……..…. p.9
2. Action Data and Working Documents Management Guidelines ……..……..... p. 10
2.1. Data Collection and Personal Data Protection ……..……..... p. 10
2.2. Data Storage and Security: Sharing and Caring Members-Only Platform…..... p.10
3. Research Outputs Authorship and Management Guidelines ……... … p. 11
3.1. Data Collection and Personal Data Protection ……..……..... p.11
3.2. Outputs Authorship ……..... p.11
3.*2.1. Reports and white papers …… …… p.11*
3.2.2. Journal articles, book chapters and monographs…… …. p.12
3.2.3. Online repositories, catalogues and directories ……..... p.12
3.3. Outputs Accessibility and Re-Usability ……. …. p.12
List of contributors.……. ….. p. 13

1. RESEARCH DATA GATHERING AND MANAGEMENT GUIDELINES

This chapter regards *research data*, which means the aggregated, recorded, retrievable information created or obtained through research or creative work. Data include but are not limited to field notes, audio- and video-recordings, transcriptions of interviews, focus groups and workshops. The chapter provides instructions on how to deal with the collection and management of these kinds of data.

1.1. Data Availability

Whenever existing data of any kind —being a written text, a spreadsheet, an image, a video- or audio-file, etc.— are *not publicly available*, it is necessary to ask authorisation for their usage. If and when authorisation is received, it is necessary to properly archive the authorising document (e.g., saving as PDF the authorising e-mail), and to share it with the Action Coordinator. In case authorisation is not granted, then refrain from using the data even if you came in possession of it.

Pay particular attention to *copyrighted material* (e.g., images). Ask authorisation for usage, pay any required fee, and safely archive documents providing evidence for both authorisation and payment.

As far as the literature repository on the public online platform (sharingandcaring.eu) is concerned, it is possible to upload there essays and books published under Open Access or with a Creative Commons license. In all other cases, *publications* should be listed with their DOI and the link to the publisher website.

1.2. Data Collection, Processing and Personal Data Protection

Before starting any research activity, researchers have the task of ensuring that each participant has understood the purpose of the activity and the procedures for data gathering and management. Furthermore, the possibility to interrupt participation at any time without providing explanation must be clearly stated. Similarly, the possibility to interrupt audio- and/or video-recording at any time must be illustrated. Participants must be also informed about the treatment of personal data, including collection (Sect. 2.2.2), processing (Sect. 2.2.3), storage (Sect. 2.3.1), retention and destruction. Names, qualifications and contact details of the staff at their disposal for further information and notices during the study must be provided to participants. Any question by the participants must be answered thoroughly. The participation of people who are not able to freely and voluntarily confirm their intention is excluded.

Tip: *Follow your institution's guidelines/rules for data management (collection, storage, protection, retention and destruction, including right to be forgotten and data erasure). Your institution may also possibly provide templates for informed consent forms. If that*

would not be the case, or you are looking to another example, you may have a look at the PIE News project template: see Appendix B of Deliverable 1.1 Project Handbook, available at: http://pieproject.eu/2016/11/29/d1-1-project-handbook/.

Informed consent is considered accomplished by field access as far as ethnographic observation and field notes are concerned. On the contrary, for interviews, focus groups and workshops, the researcher must fill in with each participant an Informed Consent Form. The Informed Consent Form, accompanied by an Info Sheet providing information on the research, its objective, its dissemination and exploitation plans, must be prepared and signed both by the participant/s and the researcher/s (one copy of signed informed consent form remains to each party). In the case of VoIP-based interviews, interviewees must be asked to send a scan copy of the signed consent form by e-mail. As for online surveys, potential participants are informed about the purposes of the survey to which they are invited to respond and asked to give their informed consent to the anonymous collection and aggregated processing of data.

Visual material such as pictures and videos require authorisation. Therefore, the issue must be properly addressed in the Informed Consent Form for interviews/focus groups/workshops, and a devoted Informed Consent Form must be prepared for visual material gathered as part of fieldwork.

1.2.2. Personal and Sensitive Data

Personal and sensitive data collection within the Action activities is to be avoided as much as possible. Personal data can be collected as by-product of research activities (e.g. collecting informed consent forms).

The European Commission (EC) considers as sensitive those data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and […] data concerning health or sex life" (Data Protection Directive (95/46/EC art. 8)[1]. The EC also details that "the term *data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership* is to be understood that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded"[2].

As for interviews, focus groups and workshops, the Action researchers should not ask questions that explicitly refer to, or may disclose, sensitive information. If, by chance, sensitive information are gathered, they must not be transcribed. The original audio- and video- files must be handled with appropriate confidentiality and technical security and must not be made publicly accessible in any case, neither upon justified and reasoned requests.

[1] Directive 95/46/EC of 24 October 1995 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 31-50.

[2] Advice paper on special categories of data ("sensitive data") of the Article 29 Working Party of 4 April 2011 (http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf), Ref. Ares(2011)444105, 20/04/2011.

If, by chance, the visual capturing/reproductions will include any personal images, especially those portraying participants' faces, they may allow others to detect biometric data. Biometric data lead to the unique identification or authentication of a natural person. The EC states that "the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means" [2, art. 51]. To avoid any possible risk, the Action researchers must not make publicly available any visual material including personal data or personal images that can endanger participants' privacy.

1.2.3. Anonymity and Confidentiality

Participants' anonymity and confidentiality must be fully guaranteed with respect to all the activities carried out and data gathered. Anonymisation takes place through the use of pseudonyms, aggregation, and any other reasonably employable means.

Interviews, focus groups and workshops are audio- and/ or video-recorded. The audio track is then transcribed. Concurrently, anonymisation must take place. *Interview, focus group and workshop transcriptions* must not contain any information or detail that may make individuals or groups identifiable. The collected data must be labelled with participant pseudonyms. The file linking participants' names as they appear in the consent forms with the respective pseudonym must be password protected and encrypted (see Sect. 2.3.1).

Personal information and details are never to be released in forms that might make subjects identifiable to any extent. To this aim, even upon request for identity disclosure by any individual participant, the researcher must assess whether this might prejudice the anonymity of other subjects, and decline the request in such a case. On the other hand, the choice concerning the disclosure or anonymisation of the names of organisations, both private and public bodies, must be discussed directly with the institutional and organisational participants of each case study. The researcher, anyway, must explicitly remind individual and collective participants of the consequences that may follow from the publication of the research data and outcomes, and what identity disclosure might imply for them.

As for *field notes excerpts and ethnographic reports* more generally, pseudonymisation must be ensured and participants' identifiabilty avoided by any means —attention must be paid not only to names but also places, addresses, recognisable/public events and activities. Moreover, confidentiality must be granted with respect to issues participants asked not to include in research reports and more generally not to disseminate by any means.

Regarding *visual material*, face blurring and other graphical means must be employed whenever such material is made public to avoid participants recognisability, except different terms of agreement has been set in the informed consent form (see Sect. 2.2.1). For confidentiality purposes, attention must be paid also to other elements of visual material, such as city or business signs, landmark buildings or monuments, and the like.

1.3. Data Storage, Security and Accessibility

This section focuses especially on the use of digital data, on their storage, and on their distribution using network connections.

1.3.1. Security Measures

All collected data, especially in their raw and hence non anonymised form, must be handled with appropriate confidentiality, accessibility controls, and technical security. In particular, all personal data collected as by-product of research activities must be kept secure and beyond the reach of unauthorised persons. Therefore:

- Data in electronic form must be stored on a secure server at the headquarters of the researcher's organisation, and access must be restricted by password protection and possibly also by encryption. Consider that data protection is enhanced by self-hosted open-source solutions and architecture.
- Data file names (e.g. of interview transcriptions or field notes) must not make reference to any personal information.
- Information that might enable data to be linked to individuals, such as the file linking participants' names to their respective code/pseudonym, must be password protected and encrypted so that access will be restricted to only those with the requisite credentials. Should confidentiality or anonymity be under threat, the file must be destroyed; a printed copy has to be generated prior to file destruction and securely kept in the researcher's safe box. Filled and signed consent forms must be held separately and must not reference the participant's code/pseudonym; they are paper-based and must be held in a locked filing cabinet on the researcher's or his/her organisation's site.

***Tip**: You may want to use Simple Secret Sharing, by Dyne.org Foundation, to protect your data. It allows you and your colleagues to securely store a text smaller than 1024 characters, such as a password, or an encryption key.*

1.3.2. Data Ownership and Data Access

Data ownership is of the researcher/s that designed and conducted research activities (ethnography, interview, focus group, workshop, survey, etc.).

All Action partners have rights to use and adapt all data collected during the project. In all cases of use, adaptation or dissemination, they are obliged to reference author/s and source of data. At the time that any dissemination project (especially publication) involving data is initiated, user must discuss co-authorship status among those who contributed to the work and reach a consensus regarding those who will be listed as co-authors. The same conditions apply to potential reuse of data for future and further research and educational purposes.

For third parties data sharing and diffusion apply only to data for which informed consent has been given, in accordance with the diffusion terms expressed by the consent, and for data in anonymised and/or aggregated form. The sharing/diffusion agreement with third parties must contain a commitment to reference author(s) and source of data.

***Tip**: If you plan to share data with third parties, use Creative Commons license conditions CC BY-SA 4.0 or CC BY-NC-SA 4.0*

All COST Action CA16121 participants will have access to data during the project period. In the general case, the raw data must be handled only by the research team involved in the

considered research activities, and made available to the rest of the Action members, if/when deemed necessary or appropriate, only in anonymous and/or aggregated form. Therefore, a) field notes, b) audio/video-recordings, and c) photos of people taken on the field without blurred faces or where people are recognisable by any other means (except different terms have been set in the informed consent form) should not be shared with other Action members if not by excerpts. It is important to ensure that materials processed from raw data e.g. interviews transcriptions, do not include personal or sensitive data (e.g. personal names).

Action members also have access to a) transcriptions of interviews, focus groups and workshops, and to b) photos without people or treated in such a way that people are not recognisable (except different terms have been set in the informed consent form). Data can be shared with other Action members through protected and encrypted Internet connections.

As for not publicly available data, accessibility is – by default – only for the Action member/s who received authorisation from the data owner. However, depending on the specific terms of agreement of such an authorisation, data may be shared with other Action members (e.g. the request was for the Action group rather than a particular member of the Action).

***Tip**: If you plan to share data that is not publicly available with other Action members or with all Action participants, declare and ask for that in your request for authorisation to the data owner.*

Third parties can request access to a) transcriptions of interviews, focus groups and workshops, and to b) photos without people or treated in such a way that people are not recognisable (except different terms have been set in the informed consent form). The decision on whether to grant or not such an access rests on the data owner/s entirely (i.e. on the researcher/s that designed and conducted research activities). It is suggested to consider several aspects: the coherence between the data and the applicants' aim, applicants' reputation, and applicants' ethical standards. Overall, the data owners evaluate the purpose and intended use of the data and then decide whether to provide an anonymous copy to the applicant or not. In fact, only after the process of anonymisation, data can be shared through protected and encrypted Internet connections.

***Tip**: In deciding whether to grant access to your data to a third party, you may ask the help of institutional Ethics Committees (e.g. from your University) and project Ethics Boards.*

1.3.3. Sharing and Caring Members Only Platform

Based on the above, data and documents that may be shared and uploaded on the Action members only platform (https://social.sharingandcaring.eu) are those that are publicly available, and not protected by copyright. These may be processed and used by other Action members.

Also data to which you received access authorisation may be uploaded and shared if you asked for that in the authorisation request, or made this request on the behalf of the whole Action or a WG of the Action (see Sect. 2.3.2 above). In this case, Action members can use data following the terms of agreement of the authorisation.

On the contrary, data that must not be shared on the Action private platform are a) field notes,

b) audio/video-recordings, c) photos of people taken on the field without blurred faces or where people are recognisable by any other means (except you set different terms in the informed consent form), and d) entire transcriptions of interviews or focus groups or workshops.

Transcriptions and more generally data in anonymous form may be shared among Action members (Sect. 2.3.2) but must not be uploaded on the Action private platform for security and privacy reasons. The rationale for this decision concerns participants' identification, as the amount of information that the considered data contain can allow others to identify single participants notwithstanding the anonymisation effort by the data owner.

Also notice that the Action private platform is covered by confidentiality agreement by all Action members (see Sect. 3).

1.3.4. Sharing and Caring Public Website

Data never to be shared on the Action public website (sharingandcaring.eu) nor to be treated as Open Research Data are raw data, and more specifically: a) field notes, b) audio/video-recordings, c) photos of people taken on the field without blurred faces or where people are recognisable by any other means (except you set different terms in the informed consent form), and d) entire transcriptions of interviews or focus groups or workshops.

Short excerpts from transcription may instead be published on the website (e.g. as part of documents that are outputs of the Action activities - see Ch. 4). You may also publicly share and possibly licensing as CC the photos taken on the field with no people or with unrecognisable people.

Data and documents produced outside the Action and not owned by any Action member, may be shared on the Action website if publicly available and not protected by copyright.

2. ACTION DATA AND WORKING DOCUMENTS MANAGEMENT GUIDELINES

This chapter regards working documents and other "Action data" such as minutes, shared primarily through the Sharing and Caring intranet platform or via dedicated Google Drive repositories.

2.1. Data Collection and Personal Data Protection

Full confidentiality applies to all working documents and data shared among Action members on the Action intranet platform, on dedicated Google Drive repositories, via e-mail or any other digital means. Full confidentiality also applies to all conversations that took place among Action members on the platform, via e-mail or any other digital means (e.g. as comments to shared documents). The breaking of confidentiality by any Action member will result in disciplinary action.

Notice that minutes may involve personal data of people taking part to the Action. For this reason, confidentiality particularly applies to minutes. Therefore, minutes must not be shared with third parties, and must not be used as research data.

2.2. Data Storage and Security: Sharing and Caring Social Platform (intranet)

The ownership of working documents shared on the platform or via other digital channels, stays with the author/s, who must be properly acknowledged whenever the document is used, adopted or disseminated. The ownership of "Action data" such as minutes belongs to the Action's Management Committee.

3. Research Outputs Authorship and Management Guidelines

This chapter considers research outputs and deliverables such as reports, white papers, publications (including journal articles, book chapters and monographs, in printed and/or digital form), online repositories, catalogues and directories.

3.1. Data Collection and Personal Data Protection

For personal data protection reasons, anonymity and confidentiality must be ensured in all research outputs. This may be achieved through pseusonymisation and by blurring faces in photographs. Whatever the means employed, the recognisability of individual persons must be avoided (see also Section 2.2.3). The only exception to this rule concerns the "online directory of people" that is foreseen in the Action Memorandum of Understanding as one of the deliverables of the Working Group 1.

Anonymity and confidentiality must be ensured also when dealing with work-in-progress research outputs that are to be shared with others on the Action intranet platform or by email or by any other means.

3.2. Outputs Authorship

3.2.1. Reports and white papers

White papers and reports —including Country Reports, Case Studies Reports and Short Stories on case studies— must contain a list of all contributors and their contribution (e.g. paper writing, data analysis, data collection, revision of version n. #).

It is important to list also contributors that are not members of the Action. This is especially the case when reporting results of already existing research conducted by researchers other than the paper or report author/s (e.g. in Country Reports).

3.2.2. Journal articles, book chapters and monographs

When aiming at publishing an article, chapter or book, in printed and/or digital form, based partially or entirely on data collected and/or analysed by other Action members, the prospect author/s of the publication must propose the data owner/s to contribute to the publication as author/s. If the data owner declines the offer, then the author/s must acknowledge her/his contribution to data collection and/or analysis (see also Section 4.2.1).

When aiming at authoring a publication based partially or entirely on research activities conducted within the Action, the prospect author/s must share the draft publication with all members for approval. The draft must be shared via the Sharing and Caring Announcements mailing list at least 10 before the last possible day for withdrawing or apply changes to the publication. Response by other Action partners is due within 48 hours. Abstention will be regarded as approval. The publication will be considered approved by the Action consortium with 51% or more of approving member countries.

3.2.3. Online repositories, catalogues and directories

Repositories, catalogues and directories published online —including, but not limited to, deliverables published on the Action public website (sharingandcaring.eu) such as the Online repository of case studies, the Catalogue of technical platforms, and the Directory of people— must include a list of contributors mentioning all involved researchers. Contributors may be listed by their roles, e.g. collection of material, organisation of material, data maintenance and updating. The list of contributors may take several forms in the considered digital space; if the repository or catalogue or directory is made downloadable, the list of contributors must be included in the downloadable file or folder.

3.3. Outputs Accessibility and Re-Usability

Material that can be shared on the Action website and are therefore publicly accessible, are the following:

- all deliverables including reports and white papers, repositories, catalogues and directories;
- publications such as journal articles, book chapters and monographs if and only if they are OpenAccess, or CC licensed, or pre-print (but check ROMEO colour for the latter option).

To favour accessibility and re-usability, Action partners are encouraged to release their publications in OpenAccess or with Creative Commons (CC) licenses such as CC BY-NC, CC BY-NC-SA or CC BY-NC-ND. Notice that CC BY-NC (Attribution-NonCommercial) and CC BY-NC-SA (Attribution-NonCommercial-ShareAlike) allow for full re-use, whereas CC BY-NC-ND (Attribution-NonCommercial-NoDerivatives) does not allow the distribution of material based on the licensed work and modified by the third party.[3]

[3] For more information, see https://creativecommons.org/share-your-work/licensing-types-examples/licensing-examples/.

LIST OF CONTRIBUTORS

Contributor	Affiliation	Contribution
Chiara Bassetti	University of Trento & CNR	First Author
Agnieszka Łukasiewicz	Instytut Badawczy Dróg i Mostów	Co-author Sect. 1.3.2