Handbook on
Ethics, Authorship
and Data Management

SharingandCaring.eu

Table of Contents

INTRODUCTION

While working on collecting and analysing cases, Working Group 1 members of our Action raised issues related to Ethics, Authorship and Data Management/Data Policy.

After researching existing guidelines in this area, we identified some publications issued by the European Commission (see, for instance, the European Code of Conduct for Research Integrity[1] and Doing Global Science: A Guide to Responsible Conduct in the Global Research Enterprise, in particular chapters 8 and 9[2]).

However, these were not well adapted to situations that might occur in COST Actions in general, and in our specific COST Action in particular. The Core Group of the Action has then decided to form a task force to establish guidelines concerning research ethics and authorship issues.

A call for interest was issued, and in March 2018, a task force on Ethics, Authorship and Data Management was created under the leadership of Chiara Bassetti.
Chiara Bassetti works for the National Research Council of Italy and the University of Trento (Italy). As an ethnographer, her research activities raised issues related to ethics and data management, as her experience comes in particular from medical emergency response and international airport security and borders control contexts, which are particularly sensitive ones. Moreover, she was the project leader of the H2020 CAPS project PIE News / Commonfare, which contributed several case studies to Working Group 1. For PIE News, she was in charge of all ethics and data management arrangements, and she authored the corresponding deliverables. The latter are currently considered as best practice examples within the EC CAPS community.

This handbook is the result of the work of this task force, and is organised in three chapters providing guidelines on: (1) research data gathering and management, (2) Action-specific data and working documents, and (3) research outputs authorship and management. For most of the guidelines, tips on how to apply them are also provided.

---

[1] http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf
[2] http://www.interacademies.org/33345.aspx

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.— is *not publicly available*, it is necessary to ask authorisation for using it. 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, one should refrain from using the data even if they came in possession of it.

Particular attention should be paid to *copyrighted material* (e.g., images). Authorisation should be requested for usage, any required fee paid, and the documents providing evidence for both authorisation and payment should be safely archived.

As far as the literature repository on the public website (sharingandcaring.eu) is concerned, priority should be given to essays and books published under Open Access or with a Creative Commons license over publications behind a pay wall. Whenever possible, *publications* should be listed with their DOI and the link to the publisher website.

1.2. Data Collection, Processing and Personal Data Protection
1.2.1. Informed Consent

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 withdraw participation at any time without providing any explanation must be clearly stated. Similarly, the possibility to ask for audio- and/or video-recording to be stopped at any time must be included. 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 available for further information and notices during the study must be provided to participants. Any question from the participants must be answered thoroughly. The participation of people who are not able to freely and voluntarily express their will should be 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,

In the case of ethnographic observation and field notes, informed consent is considered accomplished through the permission of accessing the field. On the contrary, for interviews, focus groups and workshops, the researcher must fill in an Informed Consent Form for each participant. The Informed Consent Form, accompanied by an Info Sheet providing information on the research, its objective, the 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 for 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 separate 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)[3]. 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"[4].

In the case of interviews, focus groups and workshops, the Action participants should not ask questions that explicitly refer to, or may lead to the disclosure of sensitive information if not for strong scientific reasons. In this case, or if sensitive information is gathered by chance, the original audio- and video files must be handled in a way that ensures the protection of confidentiality and technical security. In no case can these files be made publicly accessible, and in no case they can be shared with third parties (neither upon justified and reasoned requests, see Ch. 1.3.2).

---

[3]   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.

[4]   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 participants must not make publicly available any visual material including personal data or personal images that can endanger participants' privacy without their informed consent.

1.2.3.   Anonymity and Confidentiality

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

Interviews, focus groups and workshops can be 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 in such a case, decline the request. 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 of the potential implications of identity disclosure.

As for *field notes, excerpts and ethnographic reports* more generally, pseudonymisation must be ensured and participants' identifiability 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 be included in research reports and more generally not to be disseminated 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 for when different terms of agreement have 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 data collected, especially in its 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 on the premises of the researcher's organisation, and access must be restricted by password protection and possibly also by encryption. Data protection can be 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 belongs to the researcher/s that designed and conducted research activities (ethnography, interview, focus group, workshop, survey, etc.).

All Action participants have the right to use and adapt all data collected during the Action. In all cases of use, adaptation or dissemination, they are required to reference author/s and source of data. At the time that any dissemination project (especially publication) involving data is initiated, the researcher should 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 dissemination apply only to data for which informed consent has been given, in accordance with the dissemination terms expressed by the consent, and for data in anonymised and/or aggregated form. The sharing/dissemination agreement

with third parties must contain the 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 in the field without blurred faces or where people are recognisable by any other means (except for when different terms have been set in the informed consent form) should not be shared with other Action members –except for properly anonymised short excerpts from field notes.

Action members also have access to a) transcriptions of interviews, focus groups and workshops, and to b) photos without people or processed so that people are not recognisable (except for when different terms have been set in the informed consent form). It is important to ensure that the *processed data* resulted from raw data, e.g. interviews transcriptions, do not include personal or sensitive data (e.g. personal names). This data can be shared with other Action members through protected and encrypted Internet connections.

As for data that is not publicly available, accessibility is – by default – restricted to the Action participant/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 participants (e.g. the request was for the Action group rather than a particular participant in 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 processed so that people are not recognisable (except for when different terms have been set in the informed consent form). The decision on whether to grant or not such an access rests entirely on the data owner/s (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 should evaluate the purpose and intended use of the data and then decide whether to provide an anonymised copy to the applicant or not. In fact, data can be shared through protected and encrypted Internet connections only after the process of anonymisation. Personal and sensitive data cannot be shared in any case.

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's members-only platform (https://social.sharingandcaring.eu) are those that are publicly available, and that are not protected by copyright. These may be processed and used by other Action members.

Data for which authorisation to access was granted may be uploaded and shared if this permission was given in the authorisation request, or if this request was made on the behalf of the whole Action or a Working Group within the Action (see Sect. 2.3.2 above). In this case, Action members can use the data according to the terms of agreement of the authorisation.

On the contrary, data that must not be shared on the Action members-only 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 for when different terms in the informed consent form were set), and d) entire transcriptions of interviews or focus groups or workshops.

Transcriptions and more generally data in anonymous form may be shared among Action participants (Sect. 2.3.2) but must not be uploaded on the Action members-only platform for security and privacy reasons. The rationale for this rule 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, it should be noted that the Action members-only platform is covered by the confidentiality agreement agreed by all Action members (see Ch. 3).

1.3.4. Sharing and Caring Public Website

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 for when different terms in the informed consent form were set), and d) entire transcriptions of interviews or focus groups or workshops should never be shared on the Action's public website (sharingandcaring.eu) and should not be treated as Open Research Data.

Short excerpts from transcripts may be published on the website (e.g. as part of documents that are outputs of the Action activities, see Ch. 3). The photos taken in the field with no people or with unrecognisable people can be publicly shared and possibly licensed under Creative Commons.

Data and documents produced outside the Action and not owned by any Action participant, 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 concerns working documents and other "Action data" such as minutes, shared primarily through the Sharing and Caring members-only 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 participants on the Action members-only 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 participants on the platform, via e-mail or any other digital means (e.g. as comments on shared documents). The breaking of confidentiality by any Action member will result in disciplinary action.

It is to be noted that minutes may include 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 (members-only)

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 Core Group.

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 pseudonymisation 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 listed in the Action Memorandum of Understanding as one of the deliverables of the Working Group 1, and the profiles of the Action participants uploaded by each individual on the Action website sharingandcaring.eu.

Anonymity and confidentiality must also be ensured when dealing with work-in-progress research outputs that are to be shared with others on the Action members-only platform, 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 contributions (e.g. paper writing, data analysis, data collection, revision of version n. #).

It is important to list also contributors that are not participating in 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 invite 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 authoring a publication based partially or entirely on research activities conducted with support from the Action, the authors should include an acknowledgment of the COST Action CA16121 From Sharing to Caring: Examining Socio-Technical Aspects of the Collaborative Economy. Also, after publication, the author/s should add the publication to their profile/s on the sharingandcaring.eu website.

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 (<u>sharingandcaring.eu</u>) 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

Materials 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[5] for the latter option).

To favour accessibility and re-usability, Action participants 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. Note 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.[6]

---

[5]   http://www.sherpa.ac.uk/romeoinfo.html
[6]   For more information, see https://creativecommons.org/share-your-work/licensing-types-examples/licensing-examples/.

4. 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
Myriam Lewkowicz	Troyes University of Technology, France	Revision and formatting, Author of Introduction.
Gabriela Avram	University of Limerick	Final revision

We would like to also acknowledge the contributions of the Ethics Authorship and Data Management Task Force, whose ideas helped shaping this Handbook:

- Sanja Pekovic
- Agnieszka Łukasiewicz
- Minha Lee
- Stela Baltova
- Natalia Avlona