DataGo

Your situation

Well done, you've applied very good open data management practices!

You have obtained consent from participants for sharing the research materials, including their personal data, via a third-party data repository.

You have not promised participants that you would remove identifying information from your dataset. This implies that you have obtained consent to share the data "as they are".

You do not hold participants' contact details (e.g. addresses, telephone numbers).

Your legal obligations

Even if it's the best way to enable the sharing of personal data, obtaining consent still subjects you to a number of legal obligations. More precisely, to share personal data it is mandatory to:

- deposit your data in a repository that:
  - is based in Switzerland or in a country considered safe by the Federal Data Protection and Information Commissioner
  - offers storage security guarantees (e.g. servers in Switzerland/EU)
  - offers appropriate data deposit and re-use contracts
  - allows regulation of data access (e.g. for research only, with prior agreement of the data producer, after an embargo period, clearly defined re-use conditions)

- respect all the promises made in the information sheet and the consent form regarding:
  - the purposes of data collection and sharing (e.g. research, teaching)
  - the categories of data recipients (e.g. researchers only)
  - the conditions for data-sharing (e.g. embargo)
  - the use of data in publications (e.g. in a non-identifying way)
  - the data retention period

Best practices / recommandations

It is recommended to keep only the personal data that is necessary and to delete the rest. Indeed, even if you have obtained consent to share the data “as they are”, it is good practice to permanently delete all direct identifiers (including contact details) and as many indirect identifiers as possible, unless they are deemed essential (for practical or scientific reasons). Deleting highly identifying variables is a strong layer of protection, since it makes re-identification more difficult.

It is recommended to always carry out a risk assessment. If disclosing personal data might harm the participants, we recommend that you put in place additional safeguards, such as:

- replacement of identifying information with pseudonyms
- encryption of the data
- controlling and conditioning access to data (see “access control” section)
- implementation of a data use contract that sets out the re-use conditions

If the risk for participants is too high, it is recommended to contact the relevant departments within your institution and consider not sharing the data themselves. In this case, sharing just the metadata might be an option.

Access control

Data can only be shared for the purposes communicated to participants at the moment of the data collection. Therefore, data collected to address research questions can only be re-used for research purposes.

Furthermore, for sharing personal data with participants’ consent, secondary analyses must be related to the aims of the original research project. For example, re-using data collected to better understand family relationships for establishing political or religious profiles is problematic, as people have not consented to be part of such a study.

If the topic for which secondary users (researchers, students, etc.) want to access your data is very different from the one for which it was initially collected, you must require them to publish their results in a non-identifying form and to delete the data as soon as they have carried out their analyses (for example by means of an appropriate user contract). This is the only option available since without their contact details it is not possible to re-obtain participants’ consent.

For all these reasons it is strongly recommended to use a repository that allows access to be regulated, for example through deposit and re-use contracts (such as SWISSUbase).

Resources

FORS Guides: consult our guides on key data management topics, including data management planning, data protection, informed consent, data anonymisation, data sharing: https://forscenter.ch/publications/fors-guides

Data management webinar series: discover our webinars on the above topics, as well as on data documentation and security: https://forscenter.ch/datamanagement-webinar-series/

FORS archiving resources: check out our wider archiving resources: https://forscenter.ch/data-services/help-resources/

SWISSUbase resources: get access to SWISSUbase and its resources: https://resources.swissubase.ch/

Open Science at UNIL: https://www.unil.ch/openscience/en/home.html

Contact us: for any questions, get in touch with us: datago@unil.ch