



Your situation

You have informed participants of the sharing of the research materials, including their personal data, via a third-party data repository, but have not asked for their explicit consent.

You promised participants that specific identifying information would be removed from the dataset and have done so.

You continue to hold participants' contact details (e.g. addresses, telephone numbers, etc.).



Your legal obligations

Sharing research materials including personal data without the explicit consent of participants is possible if all of the following conditions hold:

- participants did not explicitly refuse the sharing of their personal data
- you have the right to possess the data; this implies that you have not promised data destruction or announced a very time-limited collection purpose
- the data are deposited 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. research only, with prior agreement of the data producer, after an embargo period, clearly defined re-use conditions)
- the data are shared for research purposes only (see “access control” section) and
- all promises made in the information sheet and the consent form are respected



Best practices / recommendations

Since you continue to hold participants' contact details, it is highly recommended to go back to them to obtain their explicit consent to sharing their personal data, unless you have imperative reasons not to do so.

It is recommended to keep only the personal data that is necessary and to delete the rest. Indeed, 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

Where no explicit consent to share personal research data has been obtained, only sharing for research purposes is possible.

In addition, secondary users must be required 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).

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/data-management-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