

Data management and data storage for surveys

This document is a guideline for data management and data storage in case data collection includes personal data. This document is still being developed. Check [this link](#) for the latest version.

*The current version of the document discusses data management & storage for data **which has a low privacy risk and is NOT subject to a DPIA.**¹*

How should I store personal data in case no DPIA is needed?

Follow the steps below.

1. Store your data on a GDPR-proof drive. This is: (i) your G-drive; (ii) your Surf-drive.
2. Pseudonymize your data.
“Article 4(5) of the GDPR defines pseudonymization as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.”
- Create a new variable with a unique value for each natural person in the data. This variable will be called ‘key’ henceforth.
- Cut your data file into two: File 1 containing the key and the personal data with which a natural person can be identified (e.g. name, address, email address). File 2 containing the key and the rest of the data.
3. File 1 needs to stay on a GDPR-proof drive and can only be transferred in a GDPR-proof way. For safety reasons, File 2 should be stored on another drive than File 1.
4. In case you need data from File 1 to perform analysis, File 1 and File 2 can be merged again. For all other analyses just use File 2.

¹ What is a DPIA?

DPIA stands for Data Protection Impact Assessment. It needs to be filled in in case of data collection with a high privacy risk. See [here](#) for a check list whether a DPIA is needed. If a DPIA is needed for your research, or if you have doubts about this, please contact XXX.