

Cognitive mechanisms of the delay-speedup and date-delay framing effects in intertemporal choice

Data management plan

Bram B. Zandbelt

bramzandbelt@gmail.com

Donders Institute, Radboud University and Radboudumc, Nijmegen, NL

Roshan Cools

roshan.cools@gmail.com

Donders Institute, Radboud University and Radboudumc, Nijmegen, NL

October 01, 2018

Abstract

This data management plan describes a dataset that will be generated to address the following research question: How does the way in which time is described influence intertemporal choice? The dataset will consist of task performance data of a maximum of 192 (but potentially fewer) human participants (one dataset of the defer-speedup framing effect and one dataset of the date-delay framing effect). The approximate total size of this dataset will be less than 1 Gigabyte. This dataset may be useful for behavioral economists, experimental psychologists, and cognitive neuroscientists interested in intertemporal choice and framing effects.

Contents

1	General information	2
2	Ethics, regulations, and policies	3
3	Planning	3
3.1	Data management roles	3
3.2	Time line	4
3.3	Data management costs	4
4	Data acquisition	4
4.1	Overview of the raw data	4
4.2	Will you use any existing data?	5
4.3	Documentation	5
4.4	Quality	6
4.5	Storage	6
4.6	Security	7
4.7	Privacy	8
5	Processing and analysis	9
5.1	Overview of the processed and analyzed data	9
5.2	Documentation	9
5.3	Quality	10
5.4	Storage	10

5.5	Security	10
5.6	Privacy	10
6	Data preservation	11
6.1	Overview	11
6.2	Documentation	11
6.3	Quality	11
6.4	Storage	11
6.5	Security	12
7	Data sharing	12
7.1	Overview of the shared data	12
7.2	Documentation	13
7.3	Quality	13
7.4	Storage	13
7.5	Security	13
7.6	Privacy	14
7.7	FAIR principles	14

1 General information

Sponsor(s) of the dataset

European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 703141 to Bram B. Zandbelt.

Producer(s) of the dataset

Donders Center for Cognitive Neuroimaging, Donders Institute, Radboud University, Nijmegen, the Netherlands.

Owner(s) of the dataset

Radboud University, Nijmegen, the Netherlands.

Keywords

Decision making, choice behavior, delay discounting, behavioral economics, experimental psychology, cognitive neuroscience, reaction time, computer model, psychological model.

Links to associated objects

Intertemporal choice task for assessing the defer-speedup and date-delay framing effects: https://github.com/bramzandbelt/itch_time_framing_task

Computational model for studying intertemporal choice and the defer-speedup and date-delay framing effects: <https://github.com/bramzandbelt/itchmodel>

Pre-registration: <https://osf.io/rzqh9/>

2 Ethics, regulations, and policies

Which regulations, guidelines, and standard operating procedures apply to the acquisition, processing, and sharing, of the data?

Data acquisition, processing, analysis, preservation, and sharing will be performed in strict adherence to the following national and international regulations and local, national, and international guidelines and standard operating procedures:

- **International regulations (European parliament and council):**
 - [European Data Protection Regulation \(Regulation EU 2016/679\)](#)
- **National regulations:**
 - [Medical Research Involving Human Subjects Act](#)
 - [Personal Data Protection Act](#)
- **International guidelines:**
 - [Declaration of Helsinki \(World Medical Association, WMA\)](#)
 - [European Code of Conduct for Research Integrity](#)
 - [FAIR Data Principles](#)
- **National guidelines:**
 - [The Netherlands Code of Conduct for Academic Practice](#)
- **Local standard operating procedures (SOPs):**
 - DCCN Data Leakage SOP

3 Planning

3.1 Data management roles

Who are the primary contributors to data management in this project?

Bram B. Zandbelt (BBZ)

Postdoctoral researcher

Donders Center for Cognitive Neuroimaging, Donders Institute, Radboud University

bramzandbelt@gmail.com

Roshan Cools (RC)

Principal investigator

Donders Center for Cognitive Neuroimaging, Donders Institute, Radboud University

roshan.cools@gmail.com

What support staff is involved in data management and how?

Other than the primary contributors, the following support staff is involved in data management:

- The **DCCN technical group (DCCN-TG)** oversees data storage, data access, and data security at the DCCN.
- **DCCN administrative personnel (DCCN-AP)** is involved in reimbursement of participants and processing of signed informed consent forms.
- The **DCCN clinical research coordinator (DCCN-RC)** and the **RU data protection officer (RU-DPO)** monitor implementation of policies on protection of personal data.

What data management roles does each of the contributors have?

role	BBZ	RC
writing data management plan	lead	support
data acquisition	lead	-
data processing and analysis	lead	-
data documentation	lead	-
data preservation	lead	-
data sharing	lead	-

3.2 Time line

When do you anticipate to acquire the data?

Data acquisition is planned to start in October 2018 and to end in December 2018.

When do you anticipate to process the data?

Data processing is planned to start in October 2018 and to end in Spring of 2019.

When do you anticipate to share the data?

Data will be shared as soon as the data processing and manuscript writing is completed. It is estimated to be the second half of 2019

3.3 Data management costs

What costs are involved in data management and how are these covered?

Costs for acquisition, processing, and analysis of the data, as well as those related to documentation of the data are covered by the grant (European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 703141 to Bram B. Zandbelt). The costs for preservation of the raw, processed, and analyzed data are covered by Radboud University and Donders Institute. The costs for sharing of the processed and analyzed data is free of charge up to 50 GB at the Zenodo research data repository. The total size of the shared data is estimated to be lower than this. Additional costs, if any, are expected to be low and will be covered by the grant.

4 Data acquisition

4.1 Overview of the raw data

What data will you acquire?

The raw dataset consists of the following:

- **Informed consent forms**
 - *Purpose*: legal compliance and record retention
 - *Data format*: hardcopy form
 - *Data size*: NA
 - *Data security classification*¹: critical

¹Following [Radboud University data security classification criteria](#)

- *Data acquisition method/system*: paper and pen
- **Screening forms**
 - *Purpose*: verification of study inclusion and exclusion criteria
 - *Data format*: comma-separated value (csv) file
 - *Data size*: < 1 MB
 - *Data security classification*: critical
 - *Data acquisition method/system*: Castor Electronic Data Capture platform
- **Personal data needed for administrative processing: name, date of birth, address, e-mail, phone number, bank account number, date of experiment**
 - *Purpose*: participant registration and reimbursement
 - *Data format*: comma-separated value (csv) file
 - *Data size*: < 1 MB
 - *Data security classification*: critical
 - *Data acquisition method/system*: SONA system cloud service
- **Pseudonimization key**
 - *Purpose*: matching of participant pseudonym and participant identity
 - *Data format*: comma-separated value (csv) file
 - *Data size*: < 1 MB
 - *Data security classification*: critical
 - *Data acquisition method/system*: standard text editor
- **Personal data needed for data processing: age and gender**
 - *Purpose*: general description of the sample
 - *Data format*: comma-separated value (csv) file
 - *Data size*: < 1 MB
 - *Data security classification*: standard
 - *Data acquisition method/system*: Castor Electronic Data Capture platform
- **Task performance data**
 - *Purpose*: measurement of behavior
 - *Data format*: comma-separated value (csv) file
 - *Data size*: 0.5 MB * 192 participants = 96 MB
 - *Data security classification*: standard
 - *Data acquisition method/system*: Stimuli will be presented with PsychoPy and custom-written code, running under Windows 7 on a Dell Precision Tower 5810 computer with a Xeon E5-1620 3.6 GHz quad core processor and 32 GB of RAM.

4.2 Will you use any existing data?

Not applicable.

4.3 Documentation

How is the content of the raw data described?

The content of the raw, experimental data is described in the following files:

- A **sample characteristics table** describes the sample in terms of age and gender.
- A **task performance codebook** documents the behavioral variables in terms of their meaning and units.

How is the context of the raw data described?

The context of the raw data is described in the following files:

- Copies of the **ethics protocol**, the **ethics committee approval letter**, the **study information package for participants**, and an **(unsigned) informed consent form** document the study approval and the study information that participants received.
- This **data management plan** describes the data and metadata gathered during research and how it will be processed, analyzed, preserved, and shared.
- A **data acquisition notebook** documents any information about the data acquisition that may be important for the processing of the data, such as events or circumstances that may affect data quality.
- A **pre-registration document** describes the data acquisition protocol.
- An **experiment handbook** contains the standardized instructions for briefing and debriefing of participants.
- A **runtime information file** documents the configuration of the stimulus presentation computer at the beginning of data acquisition.

How is the structure of the raw dataset described? What file naming conventions do you follow?

A README file that accompanies the raw dataset describes the organization of files and file naming convention. This README file is located in the project's top-level directory.

4.4 Quality

How is the quality of the raw data assured?

To assure high quality of the raw data, we will:

- use standardized instructions, so that every participant will be briefed and debriefed in the same way.
- acquire all data using the same systems (response device, stimulus presentation computer) and with standardized, tested acquisition protocols, as to limit variability.
- ensure that response devices and stimulus presentation computers are monitored by dedicated support staff (DCCN-TG).
- design the task in a way that enables identification of participants who are not paying attention (see preregistration document)
- code the task using software that allows for precise stimulus presentation and response collection timing.

How is the quality of the raw data assessed?

To assess the quality of the raw task performance data, we will inspect:

- the precision of stimulus presentation and response collection timing, using tools provided by the stimulus presentation software;
- whether participants met all pre-set task performance criteria (e.g. based on response times, etc.);
- the number of files and file sizes.

4.5 Storage

Where are the raw data stored during research?

Raw data is stored on the following devices/locations:

- **Data acquisition computers:** Task performance data are stored on data acquisition computers at the DCCN only during data acquisition. These data are removed from these computers immediately after data acquisition is completed.

- **Network-attached storage:** Personal data for data processing and task performance data are stored in project-specific directories during data processing and analysis on network-attached storage at the DCCN. These data will be removed as soon as the data is preserved and shared and the manuscript is accepted for publication in a scientific journal. The pseudonymization key is stored separately from the experimental data in the personal home directory of (one of) the researcher(s) involved in data acquisition. Once data acquisition has been completed, the pseudonymization key is handed over to the DCCN clinical research coordinator for long-term archival.
- **Project master file:** Signed informed consent forms are stored in a project-specific file in a file cabinet in a locked office at the DCCN.
- **Laptop of the researcher(s) directly involved in the project:** Task performance data with standard security classification will be stored here for data processing and analysis. These data will be removed as soon as the data is preserved and shared and the manuscript is accepted for publication in a scientific journal.
- **Castor Electronic Data Capture platform:** Screening form data and personal data needed for data processing (age and gender) are stored on the Castor platform. All data is stored on servers in the Netherlands hosted by TRUE (www.true.nl), an ISO9001, ISO27001/NEN7510 certified hosting party.
- **SONA Systems cloud service:** Personal data for administrative purposes are stored on the SONA cloud service. All data is stored on servers in Amsterdam, the Netherlands.
- **SURFdrive cloud service:** Task performance data with standard security classification will be stored here for data processing and analysis. These data will be removed as soon as the data is preserved and shared and the manuscript is accepted for publication in a scientific journal. All data is stored on servers within the Netherlands.

4.6 Security

We describe data security according to the storage device:

Who will have access to the raw data? How will you prevent unauthorized access?

- **Data acquisition computers:** Only investigators directly involved in the data acquisition of this project will have access to the data acquired on these computers. The data acquisition computers are password-protected, behind a firewall, and located in locked offices at the DCCN.
- **Network-attached storage:** Only administratively registered users with a valid account in the DCCN active directory will have access to network-attached storage. Access to the project directory on network-attached storage, where experimental data is stored, is restricted to investigators directly involved in the acquisition, processing, and analysis of the data. Access to the personal home directory on network-attached storage, where the pseudonymization key is stored, is fully controlled by and restricted to the owner of that directory. Network-attached storage is password-protected, access from outside the DCCN is restricted by a firewall, and all traffic to and from network-attached storage is encrypted. In addition, the pseudonymization key is encrypted and protected by a strong password, in line with the RU password policy. During research, the password is only known to the investigators directly involved in data acquisition.
- **Project master file:** Only authorized personnel can access the project master file that resides in a file cabinet in a locked office.
- **Laptop of the researcher(s) directly involved in the project:** Only the researcher who owns the laptop can access the research data. Several arrangements secure the laptop of the researcher(s) from unauthorized access, including password-protection, full-disk encryption, a built-in firewall, antivirus software, VPN software, and regular software updates.
- **Castor Electronic Data Capture platform:** Only researchers directly involved in the project have access to the personal data used for screening and data processing (age and gender). These data are handled strictly confidentially. All communication between users and the Castor Electronic Data Cap-

ture platform is password-protected and encrypted using SSL technology. The Castor Electronic Data Capture platform complies with all major research regulations and guidelines worldwide, including EU Data Privacy. Castor is officially certified in the field of Information Security (ISO 27001 – Standards for Information Security Assurance), the standard that describes how Information Security should be organized in a process-based manner in the context of the general business risks for the organization. More information can be found on [the website of Castor Electronic Data Capture platform](#).

- **SONA Systems cloud service:** Only researchers directly involved in the project and DCCN administrative personnel have access to the personal data used for participant registration and reimbursement. These data are handled strictly confidentially. All communication between users and the SONA Systems cloud service is password-protected and encrypted using SSL technology. SONA Systems cloud service complies with all major research regulations and guidelines worldwide, including EU Data Privacy and EU-US Safe Harbor frameworks. More information can be found on [the website of SONA Systems cloud service](#).
- **SURFdrive cloud service:** All data transmitted over the networks is encrypted. Authentication is limited to administratively registered users with a valid account at one of the universities in The Netherlands. Access to the project-specific directory (where experimental data is stored) is restricted to researchers directly involved in data acquisition, processing, and analysis.

How will you prevent loss of the raw data during research?

- **Data acquisition computers**
Immediately after data acquisition, the raw data is archived in duplicate on two password-protected and encrypted external hard disk drives that remain within the DCCN.
- **Network-attached storage at the DCCN:** A backup of the project directory and personal home directory is made on a tape robot on Radboud University campus three times per week.
- **The laptop of the researcher(s) directly involved in the project:** A backup is made on an encrypted and password-protected external hard disk drive at least once per week.
- **Castor Electronic Data Capture platform:** Backups are made four-times per day and moved to a separate geographic location daily.
- **SONA Systems cloud service:** Backups are made once per day. Backups are stored in two locations. One backup is kept in the same data center where the data reside (Amsterdam). The other backup is kept in a data center in another city in case of an unexpected facility failure. SONA Systems cloud service keeps 7 consecutive days worth of backups and archival backups from the beginning of each month for each of the last 3-6 months of service. In the case of an emergency or power failure, facilities are equipped with battery backup and diesel generators to prevent data loss.
- **SURFdrive cloud service:** SURFdrive offers a backup and recovery for a 30-day period.

4.7 Privacy

What are the privacy issues that concern the acquisition of the data, if any?

We describe data security according to the storage device:

SONA systems, Castor Electronic Data Capture platform, and SURFdrive comply with all Dutch and European privacy legislation.

- **Data acquisition computers:** No identifiable, personal (i.e. critical) data will be stored here. All experimental data will be recorded using a pseudonym.
- **Network-attached storage at the DCCN:** The pseudonymization key is encrypted and protected by a strong password, in line with the [RU password policy](#). During research, the password is only known to the PI and the researchers involved in data acquisition.
- **The laptop of the researcher(s) directly involved in the project:** No identifiable, personal data will be stored here.

- **Castor Electronic Data Capture platform:** The Castor Electronic Data Capture platform [complies with all EU data privacy guidelines](#).
- **SONA Systems cloud service:** SONA Systems cloud service [complies with all EU data privacy guidelines, including certification under the EU-US Safe Harbor Framework](#).
- **SURFdrive cloud service:** No identifiable, personal data will be stored here. SURFdrive complies with all Dutch and European privacy legislation. The data are stored safely in the Netherlands and are never made available to third parties. The location of the data is always known.

5 Processing and analysis

5.1 Overview of the processed and analyzed data

The processed and analyzed dataset consists of the following:

- **Processed task performance files**
 - *Purpose:* analysis of task performance
 - *Data format:* csv-files
 - *Data size:* < 100 MB total
 - *Data security classification:* standard
 - *Data processing software:* R (e.g. BayesFactor, ggplot) and Python (e.g. pandas, matplotlib) packages
- **Task performance descriptive statistics**
 - *Purpose:* statistical inference
 - *Data format:* csv-files
 - *Data size:* < 10 MB total
 - *Data security classification:* standard
 - *Data processing software:* R (e.g. BayesFactor, ggplot) and Python (e.g. pandas, matplotlib) packages

5.2 Documentation

How is the content of the processed and analyzed data described?

The content of the processed and analyzed data is described in the following files:

- The **pre-registration document** explains the project-specific content of the processed task performance files, descriptive statistics, and computational modeling output.
- Several **analysis codebooks** describe the meaning of values in data tables.

How is the context of the processed and analyzed data described?

The context of the processed and analyzed data is described in the following files:

- A **pre-registration document** provide a high-level overview of the data processing and analysis pipeline.
- Several **interactive notebooks** (e.g. R Markdown, Jupyter) document the data processing and analysis code in detail.

How is the structure of the processed and analyzed dataset described?

See [How is the content of the raw data described?](#) and [How is the context of the raw data described?](#).

5.3 Quality

How is the quality of the processed and analyzed data assured?

To assure the quality of the processed and analyzed task performance data, we will:

- follow best-practices in writing code for processing and analysis;
- use established software packages developed by the statistics and psychology communities (e.g. [BayesFactor](#));
- perform code reviews among project contributors.

How is the quality of the processed and analyzed data assessed?

To assure the quality of the processed and analyzed task performance data, we will:

- verify compliance with task instructions and pre-set task performance criteria;
- identify and deal with outliers.

5.4 Storage

Processed and analyzed data is stored on the following devices/locations, with specifics as in §4.4:

- **Network-attached storage:** All processed and analyzed data are stored in a project-specific directory during data processing and analysis.
- **Laptop of the researcher(s) directly involved in the project:** All processed and analyzed data are stored in a project-specific directory during data processing and analysis.
- **SURFdrive cloud service:** All processed and analyzed data are stored in a project-specific directory during data processing and analysis.

5.5 Security

Who will have access to the processed and analyzed data during research? How will you prevent unauthorized access?

See [Who will have access to the raw data? How will you prevent unauthorized access?](#) and [How will you prevent loss of the raw data during research?](#).

5.6 Privacy

If applicable, how will you anonymise or pseudonymise personal data after collection?

See [What are the privacy issues that concern the acquisition of the data, if any?](#). All data will be processed using participant pseudonyms. No identifiable, personal data will be processed.

6 Data preservation

6.1 Overview

What are the requirements regarding preservation of the data imposed by the research institute, funding agency, or scientific journal?

[Radboud University's research data management policy](#) requires that research data is preserved for at least 10 years. The European Union's Horizon 2020 research and innovation programme has not specified preservation requirements.

Which data are preserved? And for how long?

Most raw data and all processed and analyzed data will be preserved for at least 10 years from publication of the manuscript in separate collections.

6.2 Documentation

Which code and metadata will you store together with the preserved data?

All code and documentation generated during the project will be stored together with the preserved data.

6.3 Quality

Which quality assessments will you store together with the preserved data?

All quality assessment code and results will be stored together with the preserved data.

6.4 Storage

How are the data preserved? Where and for how long?

- **Raw data:** Signed informed consent forms and the pseudonymization key will be preserved in a project-specific file in a file cabinet in a locked office at the DCCN, to which only authorized personnel has access. Personal data for data processing and task performance data will be preserved in the Data Acquisition Collection of the [Donders Research Data Repository](#). Personal data needed for administrative processing will not be preserved.
- **Processed and analyzed data:** All processed and analyzed data will be preserved in the Research Documentation Collection of the [Donders Research Data Repository](#) that documents the process via which data are converted into published results. These data are preserved for at least 10 years after publication of the manuscript.

What happens to the data at the original storage locations?

- **Data acquisition computers:** All data are removed immediately after a participant's data acquisition is completed.

- **Network-attached storage:** The pseudonymization key is handed over to the DCCN clinical research coordinator for long-term archival as soon as data acquisition has been completed. All data will be removed as soon as the following conditions have been met: all relevant data have been preserved, all relevant data have been shared, and the manuscript is accepted for publication in a scientific journal.
- **Project master file:** Signed informed consent forms are archived in a project-specific file in a file cabinet in a locked office at the DCCN as soon as the study has been completed.
- **Laptop of the researcher(s) directly involved in the project:** All data will be removed as soon as the following conditions have been met: all relevant data have been preserved, all relevant data have been shared, and the manuscript is accepted for publication in a scientific journal.
- **Castor Electronic Data Capture platform:** All data will be removed as soon as data acquisition has been completed.
- **SONA Systems cloud service:** All data will be removed as soon as data acquisition has been completed.
- **SURFdrive cloud service:** All data will be removed as soon as the following conditions have been met: all relevant data have been preserved, all relevant data have been shared, and the manuscript is accepted for publication in a scientific journal.

When will the preserved data be destroyed?

Currently, the DCCN and the [Donders Research Data Repository](#) do not have standard operating procedures in place for data disposal.

6.5 Security

Who will have access to the preserved data? How will you prevent unauthorized access?

- **Raw data:** Authentication to the Donders Research Data Repository is limited to administratively registered users with a valid account at one of the universities in The Netherlands. The Data Acquisition Collection (containing the raw, experimental data) is accessible only to people directly involved in the experimental design and data acquisition in the following capacities: BZ and RC as collection managers and BZ also as collection contributor.
- **Processed and analyzed data:** The Research Documentation Collection (containing the processed and analyzed data) is accessible only to people directly involved in the processing and analysis of the data as well as other co-authors of the accompanying manuscript, if any. This ensures that all contributors and co-authors are capable of verifying the scientific work that is described in the publication. BZ and RC will be the collection managers and BZ will also be the collection contributor.

7 Data sharing

7.1 Overview of the shared data

What are the data sharing requirements imposed by the funding agency, research institute, or scientific journal?

Radboud University encourages open data. Furthermore, we have agreed to participate in the Open Research Data Pilot of the European Union's Horizon 2020 research and innovation programme.

Which data are shared?

At least the processed and analyzed data will be shared with others. This ensures that the results disseminated in the final publications can be validated. No identifiable, personal data will be shared.

7.2 Documentation

Which code and metadata will you store together with the shared data?

Documentation accompanying both the raw and the processed and analyzed data will be shared.

7.3 Quality

Which quality assessments will you share?

All performed quality assessment code and results will be shared.

7.4 Storage

Through which repository are the data shared?

The processed and analyzed data will be shared with others through the **Zenodo research data repository**. This repository is hosted by CERN in Geneva, Switzerland. Data will be retained for the lifetime of the repository. This is currently the lifetime of the host laboratory CERN, which currently has an experimental programme defined for the next 20 years at least. In case of closure of the repository, best efforts will be made to integrate all content into suitable alternative institutional and/or subject based repositories..

When will the shared data be destroyed?

Currently, the Zenodo research data repository does not have standard operating procedures in place for disposal of shared data.

7.5 Security

Who will have access to the shared data? What are the conditions under which the data are shared?

Anybody can access the shared data, provided that agreement to the conditions specified in the Data Usage Agreement that accompanies the dataset:

Use of these data is subject to the data use agreement from Donders Institute for Brain Cognition, part of the Radboud University, established in Nijmegen, the Netherlands (hereinafter referred to as the Donders Institute). I agree to the following:

1. I will comply with all relevant rules and regulations imposed by my institution and my government. This may mean that I need my research to be approved or declared exempt by a committee that oversees research on human subjects, e.g. my Institutional Review Board or Ethics Committee.

2. I will not attempt to establish the identity of or attempt to contact any of the included human subjects. I will not link this data to any other database in a way that could provide identifying information. I understand that under no circumstances will the code that would link these data to an individuals personal information be given to me, nor will any additional information about individual subjects be released to me under these Data Use Terms.

3. I will not redistribute or share the data with others, including individuals in my research group, unless they have independently applied and been granted access to this data.

4. I will acknowledge the use of the data and data derived from the data when publicly presenting any results or algorithms that benefitted from their use. (a) Papers, book chapters, books, posters, oral presentations, and all other presentations of results derived from the data should acknowledge the origin of the data as follows: "Data were provided (in part) by the Donders Institute for Brain, Cognition and Behaviour". (b) Authors of publications or presentations using the data should cite relevant publications describing the methods developed and used by the Donders Institute to acquire and process the data. The specific publications that are appropriate to cite in any given study will depend on what the data were used and for what purposes. When applicable, a list of publications will be included in the collection. (c) Neither the Donders Institute or Radboud University, nor the researchers that provide this data should be included as an author of publications or presentations if this authorship would be based solely on the use of this data.

5. Failure to abide by these guidelines will result in termination of my privileges to access to these data.

Will some of the shared data be encrypted?

None of the shared data will be encrypted.

7.6 Privacy

Are there privacy/ confidentiality issues concerning sharing data after research? If so, what are they and how will you deal with them?

Data sharing is included in the informed consent procedure at the DCCN as an opt-out construction under the condition of no direct disclosure of identifiable, personal data.

7.7 FAIR principles

How will you ensure that the shared data are findable?

According to FAIR principles, data objects can be findable if they have been assigned identifiers that are **persistent** and **unique**, and minimally contain **machine-actionable meta-data**.

Zenodo assigns all publicly available data a digital object identifier (DOI) that is **persistent** and **unique**, so that data are easily and uniquely citeable. Moreover, the Zenodo research repository provides **machine-actionable meta-data** for all data objects and a rich search syntax so that all metadata available in Zenodo can be searched.

How will you ensure that the shared data are accesible?

According to FAIR principles, data objects are accessible if it can be accessed upon **appropriate authorization**, through a **well-defined protocol**.

Zenodo's policy specifies that data "may be deposited under closed, open, or embargoed access. Files deposited under closed access are protected against unauthorized access at all levels. Access to metadata and data files is provided over standard protocols such as HTTP and OAI-PMH." All data objects will be deposited under open access.

How will you ensure that the shared data are interoperable?

According to FAIR principles, data objects can be interoperable if they are **machine-actionable**, data formats use **shared vocabularies**, and data are **syntactically parseable and semantically machine-accessible**.

The metadata in Zenodo is **machine-actionable**, because all Zenodo's metadata is exported via Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH), a low-barrier mechanism for repository interoperability. The data format use **shared vocabularies**. Data will be stored in non-proprietary formats (e.g. comma-separated value files) and processed and analyzed with open-source software (e.g. R, Python).

How will you ensure that the shared data are reusable?

According to FAIR principles, data objects are re-usable if they are accompanied by **rich metadata** and a clear **data usage license**, and meet **domain-relevant community-standards**.

As outlined in the Documentation sections above, we provide **rich metadata** that describe the dataset with a plurality of accurate and relevant attributes. As outlined in the section [Who will have access to the shared data? What are the conditions under which the data are shared?](#), the dataset comes with a clear **data usage license**. As explained under the previous item, the data organization and meta-data meet **domain-relevant community-standards**.