

Ethics in research data management

Ethical, legal and security issues

PD Dr. Olga Churakova

Open Science, Research Data Management, University Library of Bern

E-Mail: openscience@unibe.ch

SFUVET Luzern, 28.06.2022



Ethics in research data management

Outline

- Ethical issues in research on and with humans
- Data protection
- Informed consent
- Data access and data security
- Ownership & Copyright
- Licenses
- Intellectual Property Rights (IPR)
- FAIR and ethical data sharing



Research involving human beings

Personal and sensitive personal data



Personal data

- Any data that can be related to a person

Sensitive personal data

- Health, intimate sphere, “race”
- Religious, ideological, political or trade union-related views or activities
- Social security information
- Administrative or criminal proceedings and sanctions

Personality profile

- A collection of data that permits an assessment of essential characteristics of the personality of a natural person

App-based research

Data processing

Mobile Apps Issues



[Pixabay](#)

Apps running on a **participant's own device**

- pose additional threats to privacy
 - increase the complexity of data protection
 - unlikely to be entirely anonymous
 - participants may need to give permission to the app to access other services
- Clear plan, protocol, Informed Consent
 - App store release is the safest approach
 - Comply with platform controls and restrictions
 - All technical steps should be taken and verified to prevent the collection of data that is not required
 - Use encryption

Artificial Intelligence

Trustworthy



7 key requirements to AI systems:

- Empower human beings
- Resilient and secure
- Privacy and data governance
- Transparency
- Diversity, non-discrimination and fairness
- Societal and environmental well-being
- Accountability

Data Protection

General Data Protection Regulation (EU)

The [GDPR](#) is the European Union (EU) law on data protection and privacy

[Data processing Article 5.1-2](#) must meet:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability



Data protection

Federal Act on data protection (CH)

- [Federal Act on Data Protection](#) (Art. 3a, c, d) aims to protect the privacy and the fundamental rights of persons when their data is processed by **private persons (personal and sensitive personal data)** and **federal bodies**
New Swiss Data Protection Act enters into force in September 2023
- Data Protection Authorities of the Swiss Cantons – [cantonal law](#)
- [Federal Data Protection and Information Commissioner \(FDPIC\)](#)
responsible for data processing by federal bodies and private individuals
- Swiss data protection legislation is recognized by the EU-Commission



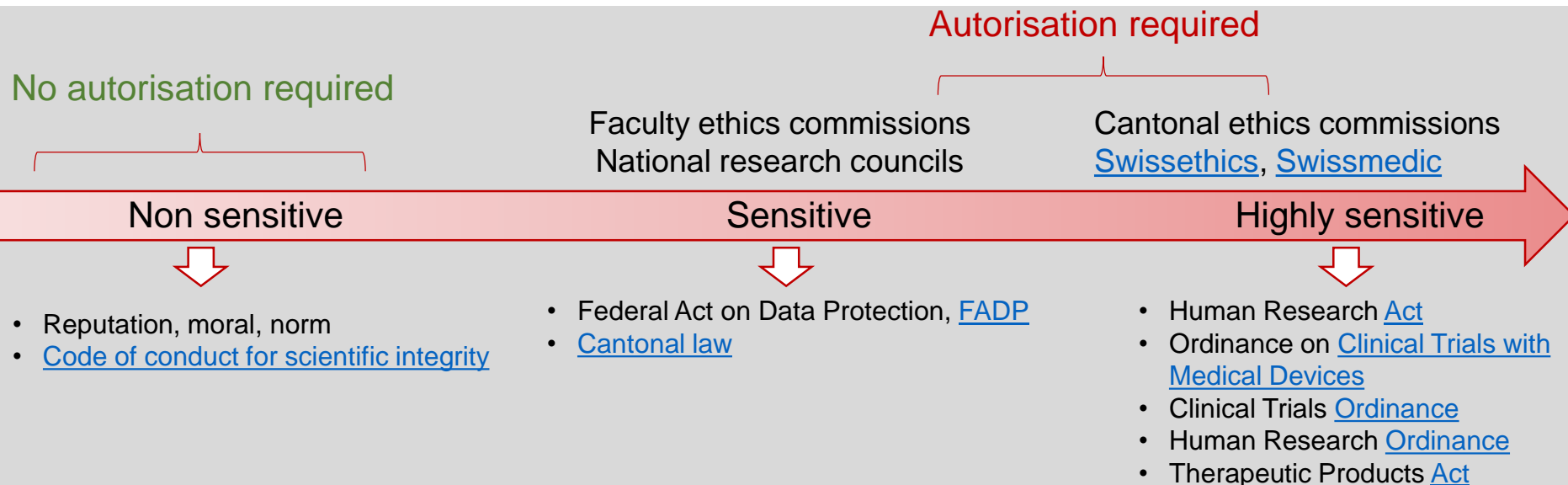
Research data management

Ethical, legal and security issues

- What is the relevant protection standard for your data? Are you bound by a confidentiality agreement?
- Do you have the necessary permission to obtain, process, preserve and share the data? Have the people whose data you are using been informed or did they give their consent?
- What methods will you use to ensure the protection of personal or other sensitive data?

Ethical issues

Research (not) requiring autorisation



SNSF guidelines

Ethics authorisation

- ❗ Copies of the authorisation or notification can be scanned and uploaded during the online submission.
- ❗ **Grants can only be paid out if all the necessary authorisations and notifications are available.** SNSF recommends that researchers **apply for these documents to the relevant authorities in parallel to the evaluation.**
- ❗ If you have received any authorisations or notifications, please upload them to the document container "Official certificates".

Ethical issues

Data access and data security


- What are the main concerns regarding data security, what are the levels of risk and what measures are in place to handle security risks?
- How will you regulate data access rights/permissions to ensure the data security?
- How will personal or other sensitive data be handled to ensure safe data storage and transfer?

Ethical issues

Before data collection



Before
data
collection



Identify a
data type
and consult

- Data Protection Office
- IT-Security
- Information security and data protection (ISDP)
- Legal advice, contracts and regulations
- Data sharing within the project with external research collaborators
- Cantonal ethics committees, research councils & commissions
- Ethical committees at the institute/faculty
- Informed Consent (IC)
- Electronic Informed Consent (eIC)

Ethical issues

Informed Consent (IC)

*“Informed Consent (IC) is a process by which a subject **voluntarily** confirms his or her willingness to participate in a particular trial, after having been informed of all aspects of the trial that are relevant to the subject's decision to participate.”*

International Council for Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use [ICH-GCP E6\(R2\)](#), 2016 Sec 1.28

Ethical issues

Informed Consent (IC)

Consent must be given

- by an unambiguous affirmative act
- **voluntarily, can revoke IC at anytime without any explanations and consequences**
- hand-written signature
- in an informed manner
- relate to the specific case and not be mixed with other declarations
- be unambiguous and easily accessible and be written in clear and plain language
- relate to all processing operations carried out for the stated purpose
- in the case of multiple purposes, all such processing purposes shall be indicated

Ethical issues

Informed Consent (IC)

A written, signed and dated IC form includes everything you plan to do with data:

- purpose, nature and extent of data processing
- duration of data storage (e.g., 10 or 15 years [SNSF guidelines](#), Art. 5.1, [swissethics](#))
- metadata remained permanently stored
- measures to protect data (anonymization, access control, etc.)
- disclosure of data to third parties / data publication and sharing

Ethical issues


Data collection



- Collect only data needed to fulfill the purpose of the study
- Principle of proportionality is one of the general principles of EU law → [Data minimisation](#)
- Describe all data which should be collected in the Informed Consent

Ethical issues

Data processing




Data
processing

- Data processing must have a well-defined purpose
- Process data only for the purpose indicated in Informed Consent
- Data must be accurate and complete
- Data must be anonymized or pseudonymized as soon as possible
- Results must be published in a way that participants are not identifiable

Ethical issues

Sensitive data

- Coding
(e.g., Code list: Name, Surname, email address, phone)
- Anonymisation
- Pseudonymisation
- Local data storage
-  NO Cloud, NO Dropbox, NO Google Drive, etc.
- Database (e.g., [REDCap](#), [secuTrial](#))



Anonymisation tools

<https://arx.deidentifier.org/anonymization-tool/>

<https://amnesia.openaire.eu/>

Ethical issues

Anonymisation

- Data is anonymized, if it cannot be related to a specific person, or re-identification requires an extraordinary effort
- Possible strategies: delete direct identifiers and / or identifying context information, aggregate, generalize, remove outliers
- Legal obligation: **data must be anonymized as soon as possible**
- As a general rule, research results may be published only in anonymised form
- Data protection regulations do not apply to anonymised data



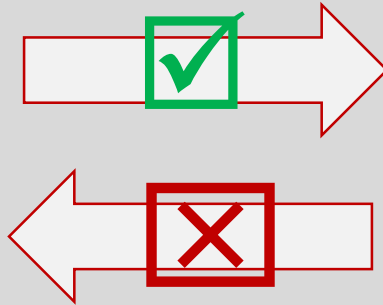
Full anonymisation might not be possible – residual risk

Ethical issues

Anonymisation

Personal information

- Name, Surname
- Birth date
- Gender
- Income
- Post code



Anonymised data

Ethical issues

Pseudonymisation

- Identifying data is replaced by an anonymous identifier (pseudonym)
- Code list allows mapping of identifiers to participants
- Code list must be kept
 - separate from data
 - securely and encrypted
 - under restricted access (PI, authorised project members)
- If anonymisation is not possible → data must be pseudonymised



Pseudonymised data ≠ anonymised data

Ethical issues

Pseudonymisation

Personal information

- Name, Surname
- Birth date
- Gender
- Income
- Post code

Code list

Participant number	Name, Surname	Age	Gender	Income	Post code
1					
2					
3					
4					

Pseudonymised data

MM4m73



Pseudonymised data is subject to data protection regulation

Ethical issues

Data collection, processing, storage



[RedCap](#)



[secuTrial](#)

[Anonymization tools: Amnesia](#), [ARX tool](#)
[Pseudonymisation tool](#)

[VeraCrypt](#) – Open Source Software
for data encryption



- Identify data security risks
- Define data access rights and permissions
- Secure data storage and data transfer agreement
- Use secure databases [REDCap](#), [secuTrial](#)
- Follow international standards
- Use secure online surveys [LimeSurvey](#), [Qualtrics](#)
- Archive for 10 or 15 years (depends on the study field [SNSF guidelines](#), Art. 5.1, [swissethics](#) and regional laws)
- Consult information security and data protection

Ethical issues

Copyright and Intellectual Property Rights

- Who will be the owner of the data?
- Which licenses will be applied to the data?
- What restrictions apply to the reuse of third-party data?

Copyright and Intellectual Property Rights

Data owner

Data/results are owned

by the institution that generate them

If two or more institutions involved →
institutes own results jointly →
jointly generated data

Written Joint Ownership Agreement

to ensure compliance with obligations for
each Institution

Each party may grant non-exclusive licence
to third parties to exploit the jointly owned
results (without any right to sub-license)

The Institutes must indicate the owner(s) of
the data/results in the final periodic report

Copyright and Intellectual Property Rights

License



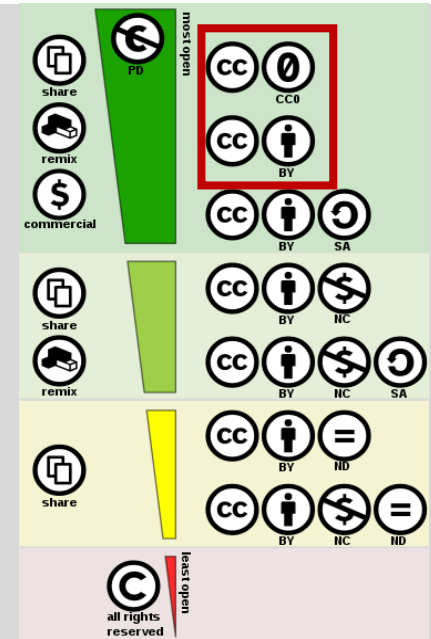
CC0 allows creators to give up their copyright and put their works into the worldwide public domain. CC0 allows reuse, remix, adapt, and build upon the material in any medium or format, **with no conditions**.



Credit must be given to the creator

CC-BY allows reuse, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator.

The license allows for commercial use.



Copyright and Intellectual Property Rights

License



- If there are **NO** ethical, legal or contractual issues
- Metadata
- Supplementary material



- [SNSF recommends](#) a CC-BY license

Copyright and Intellectual Property Rights

Licenses



CC0 license cannot be used if there are

- some forms of processed data (e.g., elaborate visualisation)
- data will be commercially exploited (patents)



CC BY license

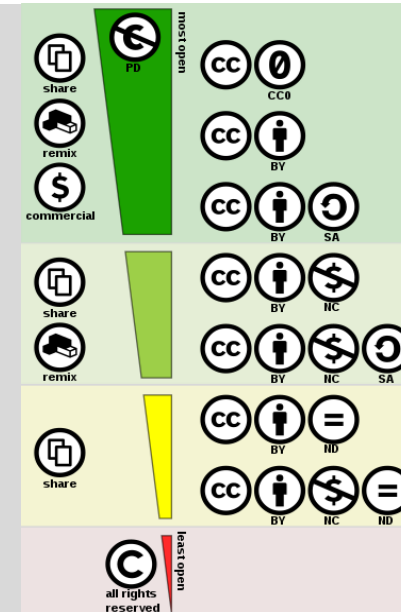
- For anonymised data or no ethical and legal issues

Copyright and Intellectual Property Rights

Third-party data

To reuse data take into account:

- Licenses
- Ownership / Copyright
- Data transfer agreement
- Written Joint Ownership Agreement



Copyright and Intellectual Property Rights

Copyright

Copyright – all rights reserved

A legal term used to describe the rights that creators have over their literary and artistic works (literature, arts, computer programs, software) [Federal act on copyright and related rights](#)

Commercial protection rights

[Patents act, PatA](#) and [Ordinance](#)

Federal Act on the Protection of [Trade Marks and Indications of Source](#)

[Info for inventors](#), [Info on research collaborations](#), [Info for business partners](#), [spin-off companies](#)



Unitecra mail@unitecra.ch

FAIR and ethical data sharing

Open research data repositories



Which data repositories can be used?

SNSF check list ([Link](#))

To find a research data repository:
www.re3data.org

FAIR and ethical data sharing

Discipline-specific data repositories

Advantages

- Best visibility
- May offer discipline-specific metadata
- Support technical requirements for specific data and vocabulary

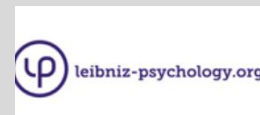
[SwissUbase](#) Social Science



[Humanities](#)



[Forschungsdatenzentrum PsychData](#)



PsychData

FAIR and ethical data sharing

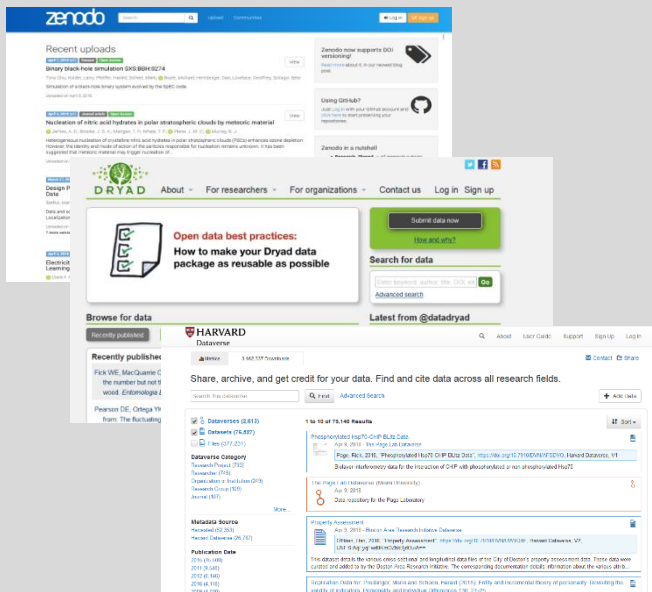
Generic repository

Advantages

- Open to all disciplines
- Easy to use

Examples

- [Zenodo](#)
- [Harvard Dataverse](#)
- [Dryad](#)



Ethics in research data management

Summary



1

- Ethics approvals
- ISDS analysis
- Information security management ([ISO](#))
- Password-protected access

2

- [Pseudonymisation tool](#)

3

- Anonymisation tool
- [Arx.deidentifier](#)
- [Amnesia](#)

4

- Closed data = No data →
- Open metadata (CC0)
- Embargo
- Restricted
- [Data Transfer Agreement](#)

Thank you
for your attention

University Library of Bern, Open Science Team
openscience@unibe.ch

u^b

^b
UNIVERSITÄT
BERN



Open
Science