RESEARCH DATA MANAGEMENT AND ETHICS

Katja Fält, Senior Specialist, PhD
Jari Friman, Information Specialist

Tampere University Library

10.5.2022

This work is licenced under Creative Commons Attribution 4.0 International License.
CONTENTS

- Why ethics matter?
- Research data management in short
- Planning ethics
- Open science and ethics
- Personal data

All photos: Unsplash
WHY ETHICS MATTER?
STARTING POINTS

• Acknowledging the requirements of research ethics is part of good data management → taking care of ethics in your own data management practices

• It is important to recognise ethical principles and data protection issues connected to data and data management
  • How to apply these principles and manage data ethically

• Research data management, research ethics and data protection should be seen as cross-cutting the entire research project

• Ethical issues may vary depending on the project but good scientific practice must be followed in all research
RESEARCH DATA AND ETHICS

Good scientific practice (The National Board on Research Integrity TENK)

• Commitment to good scientific practice is primarily up to each researcher and each member of a research team individually

• The practice of science entails quality research which produces reliable results. To achieve this, researchers must have good professional competence. Researchers’ professional competence can be seen to comprise good command of knowledge and research methodology required in each discipline and professional ethics, which together constitute good research practice.

• The methods applied for data acquisition as well as for research and evaluation, conform to scientific criteria and are ethically sustainable.

• The researcher complies with the standards set for scientific knowledge in planning and conducting the research, in reporting the research results and in recording the data obtained during the research.

• The necessary research permits have been acquired and the preliminary ethical review that is required for certain fields of research has been conducted.

• Before beginning the research or recruiting the researchers, all parties within the research project or team agree on the researchers’ rights, responsibilities, and obligations, principles concerning authorship, and questions concerning archiving and accessing the data.
RESEARCH DATA AND ETHICS

Ethical principles for research with human participants
(Finnish National Board on Research Integrity TENK guidelines 2019)

• TENK’s ethical principles in the human sciences concern research ethics. Research with human participants often requires the processing of the participants’ personal data. The guidelines have been drawn up so that the ethical principles, where applicable, support the application of the European Union’s General Data Protection Regulation (2016/679) (GDPR).
• Researchers operating in Finland must comply with the ethical principles of research with human participants.
• The guidelines are part of the scientific community’s self-regulation system.
• The ethical principles are meant to support researchers and to safeguard research participants
• There usually is no clear “right answer” to ethical questions

Note: Ethical oversight is more than legal compliance
ETHICAL PRINCIPLES IN SCIENTIFIC RESEARCH INVOLVING HUMAN PARTICIPANTS

1. Respecting the autonomy and dignity of research subjects
2. Respecting cultural heritage (material and immaterial) and biodiversity
3. Avoiding significant risks, damage or harm

Openness of research data
• Preserving the data gathered in research to make it available to other researchers is one way of ensuring open science.
• The degree of openness is determined on the basis of the data in question, taking into account both freedom of science and freedom of expression, and the protection of personal data and privacy.
• Opening the research data must be considered already at the planning stage of the research.

The ethical principles of research with human participants (2019, updated 2021)
RESEARCH DATA MANAGEMENT IN SHORT
Research data management is a part of good scientific practice

• Secures responsible and ethical research
• Helps to validate research results
• Transparency, reliability, replicability and verifiability of research

Part of the researcher skills: good data management as a default

• Reflects your managerial skills as a project leader
• Shows that you understand that your data has value

Eases the workflow

• Reduces overlapping work and makes reusing the data easier
• Organising, preserving and finding data becomes easier
• Saves time and reduces risks (data loss/data corruption, ethical or legal problems)

A data management plan (DMP) as a tool

See more: [https://libguides.tuni.fi/researchdatamanagement/plan](https://libguides.tuni.fi/researchdatamanagement/plan)
FAIR DATA

= FINDABLE, ACCESSIBLE, INTEROPERABLE, RE-USABLE

• The principles emphasise the reuse of data and good data management
• Information, publications and data, metadata and methods used and produced in the project are easily available for reuse
• Data can be FAIR even though there are limitations in its accessibility
• The principles make sure that data can be found, understood and reused
• Funders’ requirements for FAIR data (especially Horizon Europe, the Academy of Finland)

FAIR AS AN ETHICAL ISSUE?

• FAIR is connected to the skills and practices that enhance the reliability of research
  • the awareness of the FAIR principles, and the ability to apply these to the stewardship of research outputs → data reliability
  • Responsible conduct of research
• Source: SPARC Europe. Research Integrity through Open Science and FAIR Data 2019
• Ethical values of FAIR
• The European Code of Conduct for Research Integrity: Researchers, research institutions and organisations ensure access to data is as open as possible, as closed as necessary, and where appropriate in line with the FAIR Principles (Findable, Accessible, Interoperable and Re-usable) for data management
DOCUMENTING DATA

• Data documentation means the description of the content, data collection, variables and other necessary information about the data
• Enables FAIR data
• Remember to document the content and structure of the data, not results or publications
• It is possible to produce different kinds of descriptive information (text files, README-files, technical metadata, and so on)
• Document too much rather than too little
• Well-documented research data is more easily findable, accessible and reusable
• Aim:
  • Secondary users of your data can understand why, how and for what purpose the data was originally collected and how it can be used
  • You can understand and reuse your own data later on
• You can use national data documentation tool Qvain for published datasets: https://qvain.fairdata.fi/
STORING DATA

OneDrive for Business
- For staff and students.
- Capacity 1000 GB.
- Suitable for basic personal data. Use with your TUNI account.

Tuni Groups
- Similar to OneDrive for Business, especially useful for group working
- Data can be shared outside our university

Network drives
- Personal (P) and shared (S) network drives
- Capacity for staff 50 GB, students 10 GB.
- Shared network drives for research groups
- Data cannot be shared outside the university

Tailored solutions and encrypting files
- Suitable if the amount of data is big
- Suitable for sensitive data
  - Encrypting email attachments and files
  - Email encryption

Read more about personal storage space
PLANNING ETHICS
"ETHICAL LIFECYCLE"

- Planning, funding
  - Generate and collect
  - Analyse, process, store
  - Publish, share
  - Reuse

- Funders’ ethical requirements
- Ethical review
- Planning the collecting and processing of personal data
  - DMP, privacy notice, risk assessment/DPIA
- Research permits
- Agreements
- Relevant jurisdiction
- Ethical guidelines

- Personal data: data minimisation
- Informing participants + consent from participants (also to publish the data)
- Permits, terms of use

- Anonymisation
- Data selection for publication
- Reliable publication channels
- Choosing the terms of use, licenses

- Anonymisation/pseudonymisation
- Minimising the storage time of data
- Access rights to data
- Safe transfer
- Secure infrastructure for processing the data (such as remote access)
- Data encryption

- Licenses
- Terms of use
CONSIDER THESE

• Do you need an ethical review?
• Do you need a permission to carry out research or permission to use data produced by others?
• What agreements should be made (between research groups, third parties)?
• Do you use material produced by others (copyright)?
• Will you collect social media data?
  • Personal data, copyright, platform terms of use, private/public
• Will you collect personal data?
• Secondary use of health and social data?
ETHICAL REVIEW

• The Ethics Committee of the Tampere Region oversees the ethical reviews of proposed non-medical research to be carried out in the region’s universities, higher education institutions and research organisations

• Send your request for statement
  • The Ethics Committee does not grant institutional permissions to conduct a study but only issues statements of the ethical acceptability of a proposed study
  • Ethical review does not free you from responsibility

• Required documents
  1) A cover letter, 2) the research proposal, 3) an assessment of the ethical considerations by the principal investigator, 4) risk assessment, 5) impact assessment, 6) subject information sheet and privacy notice, 7) the consent form, 8) other material provided to research subjects, 9) a data management plan

The Research Data Services assist on data management plan, privacy notice, risk assessment: researchdata@tuni.fi
ETHICAL REVIEW

MEDICAL SCIENCES

• Ethical review as a default
• The ethics committees of hospital districts are responsible for ethical pre-evaluation of medical research

IN HUMAN SCIENCES
WHEN

• The research deviates from the principle of informed consent,
• the research involves intervening in the physical integrity of research participants,
• The focus of the research is on minors under the age of 15, without separate consent from a parent or carer
• Research that exposes participants to exceptionally strong stimuli
• Research that involves a risk of causing mental harm that exceeds the limits of normal daily life
• Conducting the research could involve a threat to the safety of participants or researchers or their family members or others closest to them

PERMISSIONS

• If your research or thesis topic concerns the activities of an organisation, a company or the public sector (such as a city or municipality) or you are planning to interview their staff, you must apply for research permission from the company, city or other organisation.

• You might also need to apply for a permission to use data governed or owned by third party.

• Permission procedures can vary depending on the organisation so plan the application carefully and well ahead.

  • Familiarise yourself with the needed documentation.
    • If the data is personal data, you usually need: research plan, privacy notice, data management plan, risk assessment/data protection impact assessment, ethical review, non-disclosure agreement + description of processing operations of personal data if the project involves processing special categories of personal data.

  • Ethical review should be obtained before the permission to carry out research is being applied.
AGREEMENTS AND RIGHTS

Agreeing on data

- Good scientific practise: Before the research project starts, the research project or group should agree on the rights, authorship principles, responsibilities and obligations of all parties, as well as on issues related to the storage and access rights to the materials.
- Helps to avoid disputes and conflict of interest
- Shows responsible conduct of research and good data management skills

Copyright

- Research material can include both copyrighted and non-copyrighted parts, for example, photos, drawings, videos, writings produced by research participants themselves
- If research data includes materials produced by others than researchers (for example, photographs or poems), agreements about their use must be made separately.
- It is possible to make an agreement about copyright transfer -> in principle the creator holds the right
- Use of copy-righted material created by others than research participants
  - preferably obtain written permission to use the materials

Photos: Photo by Antonio Janeski on Unsplash; Photo by Markus Winkler on Unsplash
SOCIAL MEDIA / INTERNET DATA

Can be tricky as usually involves:

- Information from humans
  - GDPR is applicable
  - Informing research subjects might be difficult
    - When the data are collected from public sources, the privacy notice and a short information sheet of the research is to be published either on the website of the research group or the website of data protection team.
- Materials produced by users
  - Copyright
- Different platforms
  - Terms of use: might have restrictions on how to collect, use and share data
  - Data ownership
- Multiple media
  - Text, images, multimedia, sound, video, games, movies, collective works, etc.
- The lines between public and private can blur
OPEN SCIENCE AND ETHICS
RESPONSIBLE SHARING

OPEN SCIENCE – RESPONSIBILITY

• Openness of research data: Ethical principles for research with human participants (Finnish National Board on Research Integrity TENK guidelines 2019)
  • Preserving the data gathered in research to make it available to other researchers is one way of ensuring open science.
  • The degree of openness is determined on the basis of the data in question, taking into account both freedom of science and freedom of expression, and the protection of personal data and privacy
  • Opening the research data must be considered already at the planning stage of the research

• The balance between openness and responsibility → always consider and plan carefully what you can and what you cannot share
  • The role of good data management is emphasised
  • “As open as possible, as closed as necessary”

• After the data has been opened, other people can use and cite the data
• The importance of metadata → enables data to be used and understood by others
  • You can publish metadata e.g. in Etsin
DATA PUBLISHING ROUTES

Prefer discipline-specific archives or repositories and follow the instructions of your funder when choosing a reliable archive. Remember that publishers might have requirements for opening data.

Data archive or a repository

- Choose a reliable archive (e.g. Core Trust Seal certified such as FSD)
- Remember, there are archives and ”archives”
- Supports FAIR
  - Curates the data
  - Offers long-term preservation
- Assigns PIDs
- Publishes metadata under a license
- Terms of use for reuse

Data journal

- A data journal publishes articles that focus on data quality or data collection methods, etc.
- Content types typically published under a CC BY license
- Assigns PIDs
- Data deposited in a repository
- Examples:
  - Springer Nature Scientific Data
  - Elsevier Data in Brief
  - Brill Research Data Journal for the Humanities and Social Sciences

Peer-reviewed scientific publication

- Many scientific publications require or recommend opening the data in a data archive or repository:
  - Increases the transparency or research
  - Makes it easier to verify results
- If you have to pay in order to get the article and the underlying data, the premise of open science is not supported
CITING RESEARCH DATA

• Accurate citing is an essential part of research ethics and good scientific practice
  • "Researchers take due account of other researchers’ work and achievements, respecting their work and giving due credit and weight to their achievements in carrying out their own research and publishing its results." (Good scientific practice and procedures for handling misconduct and fraud in science)

• Always cite your own research data if it is openly available for reuse
  • Other people reusing your data can cite it → more citations, more impact
  • Increases the visibility and findability of your data

• Always cite the research data that you have been using!
  • Gives credit to the original author
  • Other people can find the data you have used
  • Use "cite as" provided by the archive or repository
FAIR DATA SHARING CHECKLIST

• Consider already during the planning phase of your research where you will publish your data
• Use formats that are open and suitable for long-term preservation
• Create metadata
• Check that copyright or ownership does not prevent sharing data
• Define terms of reuse by a license
• Get a Persistent Identifier to your data
• Open and share your data in a data archive or data journal
• Publish metadata

(How FAIR are your data? DOI:10.5281/zenodo.1065990)

• Sharing personal data:
  • Can only be shared anonymised (pseudonymised data contains personal data)
  • Basis for processing of personal data might limit reuse (for example no consent)
  • Choose a certified data archive
  • If you cannot publish the data, publish metadata
PERSONAL DATA
WHAT IS PERSONAL DATA

Personal data refers to all information relating to an identified or identifiable natural person. Natural persons are considered identifiable, if they can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, an opinion, a job title, image or audio, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

EU's General Data Protection regulation
### PERSONAL DATA

<table>
<thead>
<tr>
<th><strong>Direct identifiers</strong></th>
<th><strong>Strong indirect identifiers</strong></th>
<th><strong>Indirect identifiers</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name</td>
<td>• Address</td>
<td>• Gender</td>
</tr>
<tr>
<td>• Personal identity code</td>
<td>• Phone number</td>
<td>• Age</td>
</tr>
<tr>
<td>• E-mail based on person’s name</td>
<td>• Car’s registration number</td>
<td>• Education</td>
</tr>
<tr>
<td>• Picture</td>
<td>• E-mail address (no person’s name included)</td>
<td>• Occupation</td>
</tr>
<tr>
<td>• Voice</td>
<td>• Web page address if page contains information about the person)</td>
<td>• Socioeconomic status</td>
</tr>
<tr>
<td>• Fingerprint</td>
<td>• Rare occupational title</td>
<td>• Income</td>
</tr>
<tr>
<td>• Dental chart</td>
<td>• Rare disease</td>
<td>• Marital status</td>
</tr>
<tr>
<td></td>
<td>• Position which only one person has at one go</td>
<td>• Language</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Nationality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Place of work</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• School</td>
</tr>
</tbody>
</table>
SPECIAL CATEGORIES OF PERSONAL DATA

Some personal data are sensitive

- Racial or ethnic origin
- Political opinion
- Religion or beliefs
- Trade union membership

- Genetic data, or biometric data processed for the purpose of uniquely identifying a person
- Health information
- Sexual behaviour or orientation
- Criminal convictions and offences

Identify and describe situations when collected personal data are sensitive as well as the legal basis for processing sensitive personal data. If sensitive personal data are processed in the research, the processing must be based on Article 9 of the General Data Protection Regulation (GDPR).
PRINCIPLES OF PROCESSING

• Personal data maybe processed only for a pre-planned and lawful purpose

• The lawful basis for the processing is in most cases is:
  • The public interest, scientific or historical research, statistical purposes
  • Data subject's consent (reversible, effects)

• **Inform the subjects** of the processing of personal data (privacy notice)

• Documentation is a way to **demonstrate** that you follow data protection law
  • Documents must be updated in the event of changes

• EU / EEA has uniform legislation (GDPR)

• Limitations in transferring data outside of EU / EEA
  • Ensure the level of data protection in outside EEA.

Photo by Chungkuk Bae on Unsplash
Processing personal data is regulated by the General Data Protection Regulation (GDPR) and by The Finnish Data Protection Act (1050/2018). The guiding principles are:

- **Lawfulness, fairness, transparency** (Choosing the processing basis)
- **Purpose limitation** (research plan)
- **Data minimisation**
- **Accuracy** (quality of data)
- **Lifespan of personal data processing**
- **Integrity and confidentiality** (access, data security)
- **Accountability**
  
  Demonstrate your compliance with data protection legislation (documentation)
PROCESSING PERSONAL DATA 2/2

• Processing personal data means
  • any operation or set of operations which is performed on personal data or on sets of personal data
  • can be done by automated means or manually
  • collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

• Storing and destruction are processing as well.
  • Requirement for information security
LAWFUL BASIS FOR PROCESSING

Tasks carried out by the data controller in the public interest.
  • Historical and scientific research and for statistical purposes
  • This is a primary recommendation when scientific research is in question.

Voluntary, specific, informed and explicit consent provided by a data subject
  • Special categories of personal data
  • Consent cannot be chosen as the lawful basis if the data subject is placed at a disadvantage, for example, because of an illness or disability, old age or if the data subject is a minor.

The data controller’s legal obligation

Exercise of the legitimate interests of the data controller or a third party if it is possible based on a so-called balance test.
DATA SUBJECTS’ RIGHTS

• Rights depend on legal basis for processing. Subjects have rights:
  • to obtain information on the processing of their personal data (timely and adequate informing)
  • to access to their data (check information)
  • to rectification of their inaccurate personal data and to have incomplete personal data completed.
  • to the erasure of their data and to be forgotten
  • to data portability
  • to restrict the processing of their data
  • to lodge a complaint with a supervisory authority (data protection ombudsman)
  • not to be subject to a decision based solely on automated processing.

• Data subjects must be informed about personal data breach

What rights do data subjects have in different situations? (Office of the Data Protection Ombudsman guides)
CONSENT

• When the processing of personal data is based on the data subject's consent and the data subject withdraws his or her consent, the data concerning him or her should be deleted unless they are immediately anonymised.

• The data processing and research based on that processing before the data subject's withdrawal is legal.

PUBLIC INTEREST

• Although the data subject withdraws his or her consent, processing of data is still possible for scientific or historical research or statistics purposes.

• The right to be forgotten does not exist when the data are processed for scientific or historical research purposes, and the right to be forgotten is likely to greatly impede or complicate such processing.

• In this case, however, the use of the data requires that the data subject’s rights be properly safeguarded. For example, data minimisation, administrative and technical information security solutions, and pseudonymisation and anonymisation of the data can be used as security measures.
THE THREE MEANINGS OF CONSENT

In research, the word *consent* has three distinct meanings:

a) *consent to participate in non-medical research* in compliance with ethical standards (see the guidelines provided by the Finnish National Board on Research Integrity TENK)
b) *consent to participate in medical research*
c) *consent as a lawful basis for processing personal data*

NOTE! An informed consent form signed by research participants does not necessarily mean that consent is the lawful basis for processing their personal data.
PRIVACY NOTICE AND RISK ASSESSMENT

• When personal data is processed participants (informants) must be informed
  • For what purpose are their data being collected
  • How their personal data are being collected, processed, used, stored, disseminated and made available

• A privacy notice is compiled in order to inform the informant
  • The form is given to the informant together with an information sheet

• Accompanied by risk assessment (or data protection impact assessment, DPIA)
  • Risk assessment will enable you to identify the level of risk and the measures you must take to ensure the secure processing of personal data
  • be aware that you must complete a concise risk assessment before processing any personal data
  • The potential risks must be assessed from the perspective of your data subjects

• Further information
  • Informing research participants (FSD’s Data Management Guidelines)
  • Data protection path of research (a template for a privacy notice there)
ASSIGN ROLES AND RESPONSIBILITIES

- A research project may involve a number of partners with different roles.
- The roles of different stakeholders and the responsibilities must be clearly defined before research begins.

<table>
<thead>
<tr>
<th>Controller:</th>
<th>Processor:</th>
<th>Joint controllers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determines the purposes and means of the processing of personal data.</td>
<td>Acts on behalf of and on the instructions of the data controller.</td>
<td>Two or more parties determine the purposes and means together</td>
</tr>
<tr>
<td>Legal entity, natural person, agency or authority.</td>
<td>Legal entity, natural person, agency or authority</td>
<td></td>
</tr>
<tr>
<td>In thesis research often a student.</td>
<td>Data controller instructs and data controller and processor sign a contract that governs the processing activities.</td>
<td></td>
</tr>
<tr>
<td>The data controller is responsible for compliance with data protection laws throughout the data lifecycle.</td>
<td>Data storage services, transcribing services, language translation services</td>
<td></td>
</tr>
<tr>
<td>• own action (including staff training)</td>
<td>• Two or more parties determine the purposes and means together</td>
<td></td>
</tr>
<tr>
<td>• service providers’ action (data processors)</td>
<td>• Two or more parties determine the purposes and means together</td>
<td></td>
</tr>
</tbody>
</table>
REQUIRED DOCUMENTATION

• Document all processing activities. Store the documentation and take care of information security. Keep documents updated.

• Examples of data protection documentation:
  • Data management plan
  • Research plan
  • Privacy notice
  • Risk assessment from the perspective of the data subject, Data Protection Impact Assessment (DPIA), prior consultation
  • Record of processing activities (often part of research data management plan or research plan)
  • Information sheet about the research
  • Contracts and guides for data processors
  • Consent forms
    • Ethical consent to participate in research
    • Consent for intervening in the physical integrity
    • Consent as a lawful basis for processing personal data
TO SUM UP

• Collect the data for specified, explicit and legitimate purposes.
• The collection of sensitive data must be based on the voluntary, specific, informed and explicit consent provided by a data subject.
• Minimise the amount of personal data (do not collect excess amount of personal data or data you do not need).
• Minimise the time you store the data.
• Protect the privacy of the informant by anonymising the data.
• Data protection tools are a necessary part of the researcher’s work and competence. Compliance with data protection regulations builds trust and lays the groundwork for future research!
BRIEF DATA PROTECTION CHECK LIST

• When planning (and processing), consider at least the following questions:

1. **Do I need to collect personal data?**
2. **Why** is personal data collected and for **what** (lawful) **purpose(s)**?
3. What is the **minimum amount** of personal data that I need?
4. How do I collect the data?
5. Do I need to ask for consent? How do I inform the subjects?
6. How do I store and maintain the data securely?
7. How long do I need to store personal data (in an identifiable form)?
8. How and when do I destroy or archive the data?

(Credit to Olli Repo and Jukka Tuomela)

Data protection check list
SECONDARY USE OF HEALTH AND SOCIAL DATA

- Secondary use = customer and register data generated in social and health care activities are used for a purpose other than the primary purpose for which they were originally saved.
  - Secondary uses are scientific research, statistics, development and innovation operations, steering and supervision by authorities, planning and reporting duty of an authority, education and knowledge management.

- Findata (Finnish Social and Health Data Permit Authority)
  - Issues permits when the study uses the social and health data of several public social welfare and health care service providers or one or more private social welfare and health care service providers.
  - Based on request and the granted permission, Findata collects data from data registrars, combines and pre-processes them (eg. pseudonymizes) and submits them for processing in a secure operating environment.
  - Findata charges for data collection, processing and storage.
  - Research projects are recommended to take into account in project planning (schedules, costs, funding) the time required for handling the data requests and data submissions.
  - Data submitted through new data requests can only be processed in an audited secure operating environment.
    - From 1 May 2022, the release of individual-level social and health data will only take place in audited secure operating environments, where they can also be analysed.
      - Findata’s Kapseli, CSC’s SD Desktop (pending audition certificate).
      - Universities do not have secure environments yet.
  - When data is needed from only one registry, a data request or data permit may be addressed directly to the registrar concerned, who processes requests/permits for its own registry data.
Research Data Services assist staff and students in matters related to research data management.

See our trainings: https://research.tuni.fi/researchdata/trainings/
Guidance and guides

Tampere University’s Open Science Policy
Research Data Management online guide
Finnish Social Science Data Archive: Data Management Guidelines
Ethical review (TAU)
Data protection path of research (TAU)
The ethical principles of research with human participants (TENK)
Finnish Advisory Board on Research Ethics (2012). Responsible conduct of research and procedures for handling allegations of misconduct in Finland
The European Code of Conduct for research Integrity (Allea)

Articles and other texts


Social Media and Research. 10 Legal and Ethical Issues to Consider. 2020. SERISS.


CONTACT

Data service
researchdata@tuni.fi