

Privacy notice in research

Instructions
Tampere University
Data Protection Officer dpo@tuni.fi
November 2020

Privacy notice

- Privacy notice is needed when personal data is processed
- Privacy notice is attached to project documentation and updated regularly. Changes are left in sight and dated.
- Issues informed in privacy notice are based on EU's General Data Protection Regulation (2016/679, "GDPR") and Finnish Data Protection Act (1050/2018)
- See also Data Protection Policy of Tampere University <https://www.tuni.fi/en/research/responsible-research> ("Data management and data protection")

Definitions: Personal data (GDPR, articles 4, 9-10)

- *Personal data* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- *Special categories of data* are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
 - Also: personal data relating to criminal convictions and offences or related security measures

Definitions: processing personal data (GDPR, article 4)

- *Processing* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as
 - 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;

Definitions: Pseudonymous and anonymous data

- **Pseudonymous data:** An individual data unit cannot be re-identified based on the pseudonymised data without additional, separate information. *Pseudonymisation* refers to the removal or replacement of identifiers with pseudonyms or codes, which are kept separately and protected by technical and organisational measures. The data remain pseudonymous as long as the additional identifying information exists.
 - Pseudonymous data is personal data!
- **Anonymous data:** An individual data unit (person) cannot be re-identified with reasonable effort based on the data provided or by combining the data with additional data points. Completely anonymous data do not exist, but with well-executed procedures one can achieve a result where individual persons cannot be identified with reasonable effort. *Anonymisation* refers to the various techniques and tools used to achieve anonymity.

Reference: <https://www.fsd.tuni.fi/aineistonhallinta/en/anonymisation-and-identifiers>

The numbers of the following slides match the numbers of the privacy notice template (TAU/TAMK)

1. Title, nature and duration of research

- Duration of research can be, e.g. funding period of a project or the period of data collection
- Duration of processing personal data may be longer than the project, if e.g. publication processes are still on-going at the end of the project
- If the exact duration of the research project cannot be specified, please indicate the factors affecting the duration thereof. Examples of such factors:
 - **Project 2019-2022. Processing personal data until the end of year 2024.**
 - **Until the publications mentioned in the publication plan have been published, and one year after the last publication.**
 - **Storage period according to the requirement of the research funder**
 - Until the dissertation of person R is accepted, estimated time of acceptance 12/2023.
- See section 17 for possible archiving of the data

2. Data controller

- *Controller* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines *the purposes and means* of the processing of personal data;
- When the principal investigator is in employment contract with Tampere University, the data controller is Tampere University Foundation sr
- When the principal investigator has an individual grant or similar funding, with no employment contract with Tampere University, the researcher is the data controller
- Data controllers can be many, which results in joint data controller. This is often the case in national or international consortiums or in co-conducted projects in which the parties decide together on the purposes and means of the processing of personal data.

3. Contact person regarding the research registry

- Contact person responds to inquiries regarding the register.
- Contact person can be the same as the principal investigator

4. Contact information of the Data Protection Officer (DPO)

- If Tampere University is the data controller, the data protection officer of Tampere University acts as the DPO, and the contact information is: dpo@tuni.fi
- If an individual researcher is the data controller, leaves this blank

5. Principal investigator or research group

- The Principal Investigator is a person assigned by the Data Controller to oversee the implementation of the research project.
- A research group may also be assigned to serve as the Principal Investigator.
- The Principal Investigator can be the same person as the contact person, in which case here you can refer to section 3.

6. Researchers

- Indicate the persons who will process the personal data collected in the project.
- In the case of joint project, indicate the persons according to their organisations.
- Indicate each person's role in processing data
- In the case of a long project, or the data processor cannot be named for other reasons, indicate the research group, department, laboratory or unit to conduct the research

7. Content of research records

- Add a description of the personal data to be processed by categories, e.g.
 - Names
 - Contact information
 - Tax district
 - Work history
 - Family relations
 - Health information
 - Genome information
 - Voice

8. Sources of personal data

- Describe from which sources data are being gained or collected.
Sources can be e.g.
 - Participant (interviews, essays)
 - Blood sample
 - Register
 - Newspaper articles

9. Purpose of processing personal data

- The purpose of processing personal data is *scientific research*
- Describe in more detail to what purposes the data are being used. For example, describe briefly the purpose/aim of the study and how the personal data processed helps to answer the research questions
- Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as *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*

10. Lawful basis for processing personal data

- In scientific research, the lawful basis is usually *Public interest or the exercise of official authority: Scientific or historical research purposes or statistical purposes*
- Processing of personal data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation requires specific lawful basis (see section 11)
- In general, one lawful basis is selected for one project. If you need to select several (Public interest AND consent), specify the basis e.g. per data set/source

11. Sensitive personal data (special categories of data and criminal records)

- “Genetic data” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- “Biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- “Data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

12. A collaborative research project: the parties and their responsibilities

- For example, the consortium parties and the responsibilities between them, especially regarding processing of personal data
- N.B. in case of joint register (section 2), separate contract is needed. Please contact: dpo@tuni.fi

13. Transfer or disclosure of data to external parties

- Personal data will be regularly transferred or disclosed to parties other than the members of the research group when, for example:
 - Data is transferred to another research group for analysis
 - An external processor is transcribing interviews or entering data in a statistical analysis software.
- When personal data is transferred or disclosed outside to the research group, one needs a data processing agreement (DPA)
- What is the difference between transfer and disclosure of data?
 - Transfer occurs e.g. within a consortium, consortium maintains the responsibility over processing
 - In disclosure, responsibility over processing personal data is transferred to the recipient, and the data controlled is changed

14. Transfer or disclosure of data outside the EU/EEA

- If personal data is transferred or disclosed outside the EU/EEA, please contact: dpo@tuni.fi
 - Survey is conducted with a programme of which server is located in country K
 - Data is transferred to country B for joint analysis of the research groups
- What is the difference between transfer and disclosure of data?
 - Transfer occurs e.g. within a consortium, consortium maintains the responsibility over processing
 - In disclosure, responsibility over processing personal data is transferred to the recipient, and the data controlled is changed

15. Automated decision-making

- Rarely used in research
- When applying for instant loan the system checks the applicant's credit

16. Data protection principles

- Register needs always to be protected with at least username and password
- For example, if personal data is transferred from person H's computer to person's F computer, data needs to be protected.
Please describe:
 - How the data is being protected during transit?
 - How the transferred files are being protected?
 - Other protection measures?

17. Processing of personal data after the research project has been concluded

- Archiving refers to post-project long-term storing of the data
- Principal investigator is responsible for appropriate processing of the data after the project; for example, that the data will be removed from the individual computers of the research group members

Data protection documentation

In addition to privacy notice, remember to take care of these:

- Risk assessment (always when personal data are being processed)
- Impact assessment (in cases when the risk assessment indicates high risk)
- Processing agreements (if personal data are being processed e.g. outside the research group)
- Joint controller agreement (in cases of several data controllers)

Questions?

Please contact: dpo@tuni.fi