Tampereen yliopisto
Tampere University

Research Privacy Notice and Thesis 30.10.2020

Data Protection Officer Jukka Tuomela
Legal Councel Olli Repo
Data Protection Specialist Anna Rytivaara

dpo@tuni.fi

Tampereen yliopisto
Tampere University

Agenda

- Privacy Notice
- Consept of ”personal data”
- When I am ”processing” personal data
- Guide to writing a research privacy notice

https://www.tuni.fi/en/research/responsible-research/data-protection

Tampereen yliopisto
Tampere University

Privacy notice and links to more information

- Free layout, does not have to be a byrocratic form. Can be more reader friedly
- Important is the content, not how it looks

- More information in FSD Data Management Guidelines
  - https://www.fsd.tuni.fi/en/services/data-management-guidelines/
  - https://www.fsd.tuni.fi/en/services/data-management-guidelines/informing-research-participants/

- EU General Data Regulation GDPR https://www.privacy-regulation.eu/en/index.htm

Tampereen yliopisto
Tampere University

Privacy Notice (GDPR, Arts. 12—14)

- A Privacy Notice is needed, when personal data is processed
- The contents of a privacy notice are based in Arts. 12—14 of the GDPR and the Finnish Data Protection Act (1050/1080)
    - The data subject (i.e. the research participant) has a right to receive information relating to the processing of their personal data in “a concise, transparent, intelligible and easily accessible form, using clear and plain language”
- The Privacy Notice is attached to the project documentation, provided to the data subjects ->
- See also the Data Protection Policy of Tampere University https://www.tuni.fi/en/research/responsible-research (”Data management and data protection”)

Tampereen yliopisto
Tampere University

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

Tampereen yliopisto
Tampere University

Examples of indirect identifiers

- IP address
- license plate / registration number,
- employment history details
- sound or video recording
- a rare hobby
- birth date
- favourite team
- profession
- names of siblings,
- blood type
- shoe size
- opinions..

Even indirect identifiers are considered personal data, i) if they can be linked to an individual or ii) an individual can be identified by a combination of indirect identifiers

It is impossible (unfortunately) to provide an exhaustive list of what constitutes personal data, even though it is frequently requested

→ Any information can be categorized as personal data

Tampereen yliopisto
Tampere University

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;

Tampereen yliopisto
Tampere University

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 (direct) 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.

  ❼Pseudonymous data is still personal data and thus subject to data protection rules!

- 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

Tampereen yliopisto
Tampere University

Orientation

- What is the subject matter of your research?
- What data are you planning on collecting and analyzing?
- Will your research involve processing of personal data?

Tampereen yliopisto
Tampere University

The numbering of the headings of the following slides matches the numbering in the research privacy notice template

- You can remove notes and instructions from the final version
- Please be aware that there is no requirement for a specific form under the GDPR; the only requirement is that the information is provided ”in a concise, transparent, intelligible and easily accessible form, using clear and plain language” -> the information is understandable to your research / data subjects

Tampereen yliopisto
Tampere University

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 requirements of the research funder
  - Until the dissertation of person R is accepted, estimated time of acceptance 12/2023.
- Follow-up studies? Provide as much information as possible in the first round; keep informing (and updating the information if necessary) for the follow-up rounds.
- See section 17 for possible archieving of the data

Tampereen yliopisto
Tampere University

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 usually 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 controllership. This is often the case in national or international consortiums or in co-conducted projects in which the parties decide together the purposes and means of the processing of personal data
  - Does participation in a consortium automatically indicate the existence of a joint controllership situation?

Tampereen yliopisto
Tampere University

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

Tampereen yliopisto
Tampere University

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, remove this section

Tampereen yliopisto
Tampere University

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.

Tampereen yliopisto
Tampere University

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 research team cannot be named for other reasons, indicate the research group, department, laboratory or unit to conduct the research

Tampereen yliopisto
Tampere University

7. Content of research records

- Add a description of the personal data to be processed by categories, e.g.
  - Names
  - Contact information
  - Survey answers (regarding xx)
  - Work history
  - Family relations
  - Health information
  - Genome information
  - Voice
  - Interviews

Tampereen yliopisto
Tampere University

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
  - Company, public authority
  - Newspaper articles

Tampereen yliopisto
Tampere University

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

Tampereen yliopisto
Tampere University

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

  Master’s and bachelor thesis: lawfull basis is more often consent

- 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

Tampereen yliopisto
Tampere University

10. NB. ”Consent” in research

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

a) *consent to participate in non-medical research* in compliance with applicable ethical standards (see the guidelines provided by the Finnish National Board on Research Integrity TENK)

b) consent to participate in medical research (Finnish Medical Research Act, 6 §, 9.4.1999/488)

c) consent as a lawful basis for processing personal data (the EU’s General Data Protection Regulation, article 6:1a).

→ An informed consent form signed (to participate in a study) by research participants does not necessarily mean that consent is the lawful basis for processing their personal data.

→ If you rely on consent as the lawful basis for processing, ensure that the provided consent meets the GDPR requirements.

- Relying on consent as a lawful basis for data processing is not without risks, because further processing activities must be stopped if consent is withdrawn. The data collected about the individual may have to be destroyed if he or she withdraws consent.

Tampereen yliopisto
Tampere University

10. Requirements for consent

The consent must be

- ✓ specified
- ✓ informed
- ✓ freely given, and
- ✓ unambiguous indication of the data subject's wishes.

- When processing personal data of special categories (=sensitive data), the consent must be explicit and documented
- Data subjects can give their consent for predefined, specific and lawful purposes. If the purpose of processing personal data changes, you need to ask for a new consent before starting processing. Also when post-project reuse of data is wanted
- It shall be as easy to withdraw consent as to give it.

Lähde: https://tietosuoja.fi/en/consent-of-the-data-subject

Tampereen yliopisto
Tampere University

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;

Tampereen yliopisto
Tampere University

11. Sensitive personal data (special categories of data and criminal records) (art 9)

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purpose

e) processing relates to personal data which are manifestly made public by the data subject;

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

- shall be proportionate to the aim pursued,
- respect the essence of the right to data protection and
- provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Tampereen yliopisto
Tampere University

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), a separate contract is needed. Please contact: dpo@tuni.fi

Tampereen yliopisto
Tampere University

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 (joint controllers); consortium members maintain the responsibility over processing
  - In disclosure, responsibility over personal data is transferred to the Recipient (acting as an independent controller defining the means and purposes)

Tampereen yliopisto
Tampere University

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

Tampereen yliopisto
Tampere University

15. Automated decision-making

- Rarely used in research
- E.g. an instant loan the system checks the applicant's application

Tampereen yliopisto
Tampere University

16. Data protection principles

- Data “at rest”: Register needs to be protected with information security measures, e.g. at least a username and a password
- Data “in transfer”: e.g. when personal data is transferred from person H’s computer to person F’s computer, data needs to be protected. Please describe:
  - How the data is being protected during transit?
  - How the transferred files are being protected (secure e-mail, encryption)?
  - Other protection measures?

Tampereen yliopisto
Tampere University

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

- Archieving 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

  - Erasure
  - Anonymisation

Tampereen yliopisto
Tampere University

Questions?

Please contact: researchdata@tuni.fi