

# Data protection in thesis

13.10.2021

Data protection officer Tiina Kangas  
Data protection lawyer Susanna Halmela  
Senior specialist Jukka Tuomela  
Data protection specialist Anna Rytivaara

[dpo@tuni.fi](mailto:dpo@tuni.fi)

# Today's program

- What is data protection
- Data protection in thesis
- Privacy notice – what, why, how?
- Links for more information

# Data protection in Tampere Universities

- Data protection is the process of **protecting personal data**.
- Data protection is a fundamental right and safeguards the rights and freedoms of data subjects (=research participants) when their personal data is processed.
- Every community member's duty
- The principals have agreed on a common [data protection policy](#)
- Data processing laws set out the principles for the lawful processing of personal data.
- The processing of personal data must always be based on law.

# Data protection legislation in a nutshell

- EU's General Data Protection Regulation (GDPR)
  - To be applied in all EU/EEA countries
  - In some parts has flexibility for national interpretations
- Data Protection Act (1050/2018)
  - National interpretations in Finland
  - Definition of "public interest"
    - Scientific and historical research
    - Data archiving
- Act on the Openness of Government Activities (621/1999) "Openness Act"
  - Permission to access documents, also classified documents and registers

# Data protection in Tampere Universities

- Data security policy and other regulations
- In intranet:
  - [Data protection and data security](#)
  - [Research IT](#)
- In the public website: data protection in research
  - <https://www.tuni.fi/research-data-protection>
- FSD: [Data Management Guidelines](#)
- Training by Research data
  - [Recording and slides of the past trainings](#)

# The role of the supervisor

- Thesis supervision
  - For supervisors: <https://intra.tuni.fi/en/handbook?page=20506>
  - For students: <https://intra.tuni.fi/en/handbook?page=2771>
- Important role of the supervisor
  - thesis supervisor (or teacher in the case of other student assignments) must advise students on the appropriate processing of personal data
  - thesis supervisor should consult with the student in advance to determine the purpose, scope and manner of data processing activities → **documenting the plan**
  - The types of personal data that a student may be allowed to process will depend on the stage of his or her studies. Does the student have required ability to process personal data in accordance with the regulations?

## 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

## 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**

→ Any information can be categorized as personal data



# 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.
  - **Pseudonymous data is 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>

# Principles of processing personal data

When processing personal data, the following principles are to be applied:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation (processing period)
- Integrity and confidentiality (access to data, data security)
- Obligation to demonstrate that the principles are being applied

More detailed descriptions: <https://www.tuni.fi/research-data-protection>

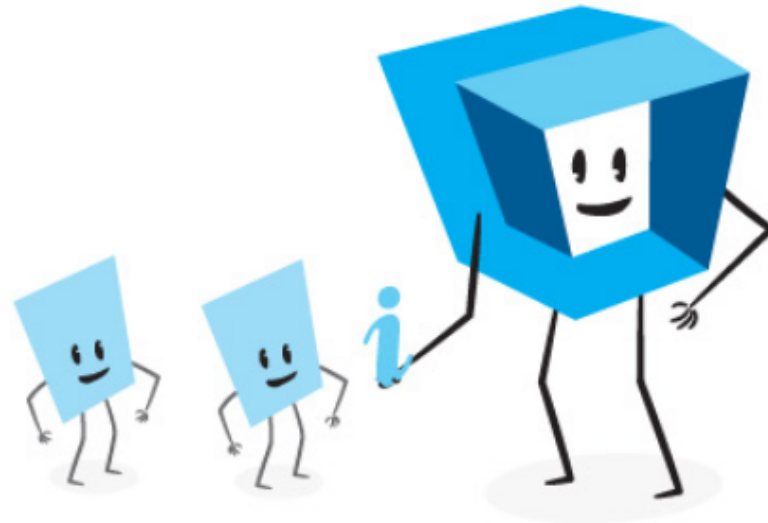
# INFORMING RESEARCH PARTICIPANTS ABOUT THE PROCESSING OF THEIR PERSONAL DATA

## 1. General

Next

Informing research participants about the processing of their personal data is a crucial part of the transparency principle laid down in the General Data Protection Regulation of the European Union (GDPR). Based on the provided information, the participants must understand how their personal data are being collected, used, stored, disseminated or otherwise made available, or otherwise processed. The significance of forward planning is emphasised in the processing of personal data. Informing research participants can be challenging without thorough consideration of all phases of the research and the applicable regulatory framework before starting research. On the other hand, if personal data processing has been planned thoroughly and systematically in advance, informing participants becomes much more straightforward.

The rules of informing research participants about the



### On this page

-

1. General

2. Clarity requirements and form of the information

# Privacy Notice (GDPR, Arts. 12—14)

- A Privacy Notice is needed, when **personal data** is processed
- The purpose of the notice is **to inform the participant**
- 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” (GDPR, art 12.1)
- Templates available for scientific research and for theses
- The purpose of templates is to provide sufficient information (content) for the participant
- Sections irrelevant for research in question are to be erased
- Content matters, not the form
- Templates: <https://www.tuni.fi/research-data-protection>

# Template for privacy notice in thesis

- More concise template of privacy notice
- Available in Finnish and English
- Both the thesis and the role of the supervisor noted
  - Can be applied in thesis research (students as the data controller)
  - University as the data controller (supervision and assessment)

## 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. This means that the student is responsible for the duties set for the data controller in the data protection legislation.
- When thesis is conducted as part of a preplanned university project, it is possible that the university acts as the data controller for the thesis.
- When thesis is conducted on behalf of a company (customer-funded research) or if you are employed by a company, it is possible that the company acts as 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

## 9. Purpose of processing personal data

- The purpose of processing personal data is thesis or scientific research
  - Criteria for scientific research include publishing the results and review of the scientific community, autonomy of research and adequate qualification of the author
- Describe the content of the research and what the data are used for. For example, describe the purpose of your thesis and how the personal data will help in answering the research questions.
  - Remember that you can also process data you really need to answer your research questions

## 10. Lawful basis for processing personal data

- In thesis research, the lawful basis is usually *consent*
- In scientific research, the lawful basis is usually *Public interest or the exercise of official authority: Scientific or historical research purposes or statistical purposes*
  - Sometimes it is advisable to ask for a consent in cases that involve intervening in the physical integrity (smart band, smart ring, physical activity belt)
- 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



## 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.

# 10. Requirements for consent

Consent to be valid, it needs to be

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

- 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.
- It shall be as easy to withdraw consent as to give it. Withdrawal of consent does not affect the analysis that have already been conducted but prevents any further analysis of the data.

Source: <https://tietosuoja.fi/en/consent-of-the-data-subject>

# 1. Duration of processing

- Personal data can only be stored in a form which enables the identification of a person no longer than it is necessary to fulfil the purpose of processing
- If the exact duration cannot be defined, give a factor affecting the duration thereof. Examples:
  - Until the thesis has been accepted, assessed acceptance 12/2023.
  - Until the publications listed in the publication plan of the project have been published.
- If you are planning to use the same data in your next thesis:
  - Processing activities need to be planned already during the earlier thesis and the participants need to be informed about the further processing of their data, or
  - You need to ask for a new consent for a new purpose.
- See section 17 for possible archiving of the data

## 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
- If the data is collected by interviewing or questionnaires, describe the main topics or themes of them
- Remember that personal data needs to be necessary to fulfil the aims of your research

# 11. Special categories of data and criminal records (sensitive personal data) (GDPR, art 9)

Processing of personal 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 shall be prohibited. Exceptions are:

- a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
- 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
  - which 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.

## 8. Sources of personal data

- Describe from which sources data are being gained or collected. Sources can be e.g.
  - Participant (interviews, essays, questionnaires, blood samples)
  - Public documents
  - Registers
- If several sources, specify what information is gained from which source
  - Blood samples participants, health information from registers, tax records from the tax officer
  - Immigration history from Migri, family history from participant families, foster care documents from child protection services

## Concise risk assessment

- The goal is to identify the following already at the planning stage:
  - **the risks** that the processing activities may pose to data subjects, and
  - **the measures** that must be taken to ensure processing activities are carried out in compliance with data protection regulations.
- The risk assessment must be completed before processing activities begin.
- The risks of each processing activity must be assessed from the the data subjects' perspective.
  - The assessment does not focus on the perspective of the research project, organisation or individual researcher.
- The risk assessment must be documented. You must assess and record the following points:
  - What freedoms and rights of data subjects could be at risk?
  - What damage could be incurred by data subjects from the processing of their personal data?
  - What measures can I take to eliminate or reduce the risks?

## Data protection guidelines and instructions in TUNI websites

- <https://www.tuni.fi/research-data-protection>
- Document library
  - **Templates (privacu notice, risk assessment, joint controller agreement)**
- FAQ-section
- In the Intranet
  - **Handbook Security and safety at work → Data protection and information security**
  - <https://intra.tuni.fi/en/handbook/2686/2725>
- [Data Management Guidelines](#) by FSD
- Training by Research data
  - [Recording and slides of the past trainings](#)



# Discussion and questions

Ota yhteyttä: [researchdata@tuni.fi](mailto:researchdata@tuni.fi)

# Data protection legislation in a nutshell

- EU's General Data Protection Regulation (GDPR)
  - To be applied in all EU/EEA countries
  - In some parts has flexibility for national interpretations
- Data Protection Act (1050/2018)
  - National interpretations in Finland
  - Definition of "public interest"
    - Scientific and historical research
    - Data archiving
- Act on the Openness of Government Activities (621/1999) "Openness Act"
  - Permission to access documents, also classified documents and registers
  - The secondary use of health and social data (Act 552/2019)

# Data protection in Tampere Universities

- Presidents have confirmed a joint [data protection policy](#)
- Data security policy and other regulations
- In intranet:
  - [Data protection and data security](#)
  - [Research IT](#)
- In public website: data protection in research
- In the public website: data protection in research
  - <https://www.tuni.fi/research-data-protection>
- FSD: [Data Management Guidelines](#)
- Training by Research data
  - [Recording and slides of the past trainings](#)

## 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;

## 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?
- Rather than transferring the data, a shared storage or virtual desk?
- IT for research: <https://intra.tuni.fi/en/handbook/2677/2731>

## Other data protection document

- Concise risk assessment (template available)
  - Data protection impact assessment (DPIA) if needed
- Data processing agreement (DPA)
- Joint controller agreement