

Data protection impact assessment (DPIA) [name of the research project]

Contents

[Data protection impact assessment 4](#_Toc66696687)

[1. General description of processing 4](#_Toc66696688)

[1.1. Basic information about the research 4](#_Toc66696689)

[1.2. Scope of processing activities 4](#_Toc66696690)

[1.3. Categories of personal data to be processed 4](#_Toc66696691)

[2. Necessity and proportionality 6](#_Toc66696692)

[2.1. Purpose limitations 6](#_Toc66696693)

[2.2. Data minimisation 6](#_Toc66696694)

[2.3. Transparency and timely communication 7](#_Toc66696695)

[2.4. Consent management (if lawful basis for processing is consent) 7](#_Toc66696696)

[2.5. Storage limitation and anonymisation or pseudonymisation 7](#_Toc66696697)

[2.6. Data subjects’ rights and exemptions 8](#_Toc66696698)

[2.7. Integrity, confidentiality and availability 8](#_Toc66696699)

[2.8. Transfer of personal data and the recipients 8](#_Toc66696700)

[3. Risks associated with the processing 10](#_Toc66696701)

[3.1. Identifying the risks associated with processing personal data 10](#_Toc66696702)

[3.2. Unauthorised disclosure of or access to personal data 10](#_Toc66696703)

[3.3. Destruction or unauthorised modification of personal data 11](#_Toc66696704)

[3.4. Loss or alteration of personal data 11](#_Toc66696705)

[3.5. Summary 11](#_Toc66696706)

[4. Stakeholder comments 11](#_Toc66696707)

[4.1. Comments by the data protection officer 11](#_Toc66696708)

[4.2. Comments by other stakeholders 12](#_Toc66696709)

[5. Summary 12](#_Toc66696710)

**Stages of the data protection impact assessment (DPIA):**

|  |  |  |  |
| --- | --- | --- | --- |
| Stage | Date | Name | Comments |
| A draft version of the DPIA is completed  | Enter the date | Name | Comments |
| The data protection officer is consulted | Enter the date | Name | Comments |
| The DPIA is completed | Enter the date | Name | Comments |

**Appendices to the data protection impact assessment:**

Appendix 1: Research privacy notice

Appendix 2: Basic risk assessment

(Appendix 3: Records of processing activities if not included in the privacy notice)

(Appendix 4: Balancing test if the lawful basis for processing is legitimate interest)

(Appendix 5: Data flow map)

# Data protection impact assessment

# Description of processing activities

### Basic information about the research

* + 1. Name of the research study or other identifier

Name of the research study or other identifier

* + 1. Principal investigator and research group

Principal investigator: Principal investigator

Contact information: Principal investigator’s contact details

Research group: Research group or field of research

### Scope of processing activities

Number of research subjects: Number of research subjects (estimate)

Planned duration of the research study: start date— end date

### Categories of personal data to be processed

* + 1. **Categories and sources of personal data**

*The term 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 or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.*

What types of personal data will be processed during the research study? Describe the personal data that will be processed (types of personal data), whose personal data will be processed (groups of data subjects) and how or from whom personal data will be collected (sources of personal data). You must also indicate the purposes for processing personal data (purpose of processing) and the lawful basis for each processing activity (lawful basis of processing).

|  |
| --- |
| Personal data collected from data subjects |
|  |

|  |
| --- |
| Personal data collected from other sources |
|  |

* + 1. **Processing special category personal data**

*The term special category personal data refers to data that reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data (when used for identification purposes), health data, or data concerning his or her sexual behaviour or orientation.*

Will your process special category personal data (sensitive personal data) or data concerning criminal convictions or offences in the course of your research? Describe the personal data that will be processed (types of personal data), whose personal data will be processed (groups of data subjects), how or from whom personal data will be collected (sources of personal data). Also indicate the purposes for processing personal data (purpose of processing) and the lawful basis for each processing activity

(lawful basis of processing).

|  |
| --- |
| Special categories of personal data and data concerning criminal convictions |
|  |

* + 1. **Description of processing activities**

Draw up a systematic description of the nature, scope, context and purpose of processing personal data. Consider the entire lifecycle of personal data from the collection of data to the destruction/archiving of data.

The description should indicate why and how personal data will be processed during your research study. Address especially the following questions: How will you process personal data? Where will you store personal data? Who will take part in processing personal data, and what are their respective roles and responsibilities? How will data be shared with possible other stakeholders involved in the processing activities? What will happen to the data after your study has been completed?

If you have prepared a separate data flow map or description of your processing activities, you can refer to these documents in this section.

|  |
| --- |
| Description of processing activities |
|  |

* + 1. **Codes of conduct**

Will your processing activities be carried out in compliance with specific codes of conduct as referred to in article 40 of the GDPR?

|  |
| --- |
| Indicate the codes of conduct, if applicable.  |
|  |

# Necessity and proportionality

### Purpose limitations

*Personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with the original purposes.*

What are the specific purposes for collecting and processing personal data? How will you ensure that personal data will not be processed for any other purposes?

|  |
| --- |
| Demonstrate adherence to the purpose limitation principle |
|  |

### Data minimisation

*Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

How do you ensure that only relevant and necessary personal data, which you need to fulfil your specified purposes, will be collected and processed in the course of your study?

|  |
| --- |
| Demonstrate adherence to the data minimisation principle |
|  |

### Transparency and timely communication

*Data subjects must be made aware of how the personal data you hold about them will be processed and used. All information and communications must be provided in a concise, transparent, intelligible and easily accessible form using clear and plain language.*

What information will you provide to data subjects about your processing activities? How will you provide the information about your processing activities? When will you provide this information?

|  |
| --- |
| Describe how the data subjects will be informed of the processing |
|  |

### Consent management (if lawful basis for processing is consent)

If you ask your data subjects to provide consent for the processing of their personal data, how will you handle the consent management process? How will data subjects provide their consent? How will you record their consent? How can data subjects withdraw their consent?

|  |
| --- |
| Describe the consent management process if the lawful basis for your processing activities is consent (GDPR Art. 6.1(a)). |
|  |

### Storage limitation and anonymisation or pseudonymisation

*Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which their personal data are processed. Data controllers must set deadlines for the deletion of personal data or for the periodical review of personal data to ensure that personal data is not held for any longer than is necessary.*

How have you set a retention period for the personal data you will collect or specified the criteria for setting the retention period? Have you considered possible further use of personal data when setting the retention period? How and when will you carry out anonymisation or pseudonymisation procedures?

|  |
| --- |
| Storage limitation and anonymisation or pseudonymisation |
|  |

### Data subjects’ rights and exemptions

*Depending on the lawful basis for processing, data subjects may have the right to obtain a copy of their personal data (right of access), the right to rectification, the right to erasure (the right to be forgotten), the right to restrict processing, and the right to object to the processing of their personal data.*

Describe the process for ensuring the enforcement of data subjects’ rights. Who is identified as the contact person for inquiries? How will you ensure that information requested by data subjects can be provided and that their other requests can be fulfilled? How will you document and store requests and responses?

|  |
| --- |
| Process for ensuring the enforcement of data subjects’ rights |
|  |

Under certain circumstances, data protection laws allow an exemption from particular data protection provisions. Are there exemptions that apply to your study?

|  |  |
| --- | --- |
| Specify the exemption  | Reason for exemption |
|  |  |

### Integrity, confidentiality and availability

*Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.*

Describe the measures (including the information security measures) that you will take to ensure the integrity and confidentiality of personal data during the different stages of processing throughout the data lifecycle.

|  |
| --- |
| Integrity and confidentiality during the data lifecycle |
|  |

### Transfer of personal data and the recipients

* + 1. **Joint controllers**

*If there are at least two data controllers who jointly determine the purposes and means of processing personal data, they are referred to as joint controllers.*

If multiple data controllers participate in the processing of personal data as joint controllers, indicate their names, contact details, their role in the processing activities, and the contact details of their designated data protection officer, if applicable.

|  |
| --- |
| Joint controllers |
|  |

* + 1. **Data processors (subcontractors)**

*The term data processor refers to a person or an organisation that processes personal data on behalf of and on the instructions of the data controller.*

If data processors (such as providers of survey, analysis or transcription services) participate in the processing activities, indicate their names, contact details, their role in the processing activities, and the contact details of their designated data protection officer, if applicable.

|  |
| --- |
| Data processors |
|  |

* + 1. **Third parties and data recipients**

Will personal data be transferred or disclosed to third parties? Will third parties have access to personal data?

|  |
| --- |
| Other parties involved in the processing activities or receiving personal data  |
|  |

* + 1. **Transfer of personal data outside of the European Economic Area (EEA)**

*Any transfer of personal data outside the EEA must be carried out in compliance with the GDPR requirements.*

If personal data will be transferred outside the EEA, where will data be transferred? What GDPR-compliant transfer mechanism (Chapter V of the GDPR) will be applied to the transfer?

You can also state this information in sections 2.8.1—2.8.3 above based on the role of each data recipient.

|  |  |  |  |
| --- | --- | --- | --- |
| Type of personal data | Recipient | Location | Transfer mechanism  |
|  |  |  |  |

# Risks associated with the processing

### Identifying the risks associated with processing personal data

Assess the risks that your processing activities may pose to data subjects, especially the risks arising from 1) unauthorised disclosure of or access to personal data, ii) unintentional or unauthorised destruction or modification of personal data, and iii) the loss or alteration of personal data. How would you rate the severity of the possible harm or damage if the risks are realised? How would you rate the likelihood of the risks? Potential risks include, for example:

* unauthorised re-identification of pseudonymised data or loss of control over the use of personal data,
* identity theft or fraud, financial loss,
* other social disadvantage, such as reputational damage, or
* physical harm (especially when processing special category data).

Identify measures that you can take to mitigate the risks. You can consider, for example, the following questions:

* How will you restrict access to personal data to ensure that only individuals who need to process this data for research purposes are able to gain access?
* Where will personal data be stored? How will you securely store personal data to maintain the integrity and confidentiality of data?
* How will personal data be securely transferred during different stages of the study?

Type your comments in the tables below. You can refer to your earlier risk assessment as well as the mitigation measures listed in Section 2 of this DPIA.

### Unauthorised disclosure of or access to personal data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Likelihood | Severity  | Mitigation | Remaining risk[[1]](#footnote-1)  |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |

### Destruction or unauthorised modification of personal data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Likelihood | Severity  | Mitigation | Remaining risk  |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |

### Loss or alteration of personal data

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Likelihood | Severity  | Mitigation | Remaining risk  |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |
|  | Select | Select |  | Select |

### Summary

Overall assessment of the data protection risks: Select

# Stakeholder comments

### Comments by the data protection officer

Data protection officer’s comments:

Name: Click or tap here to enter text.

Date: Click or tap to enter a date.

|  |
| --- |
|  |

### Comments by other stakeholders

Stakeholder comments:

Stakeholder group: Click or tap here to enter text.

Name: Click or tap here to enter text.

Date: Click or tap to enter a date.

|  |
| --- |
|  |

# Summary

The planned measures for eliminating or controlling data protection risks are adequate and therefore the processing activities are not likely to pose a high risk to the rights and freedoms of data subjects (to be filled in by the person who carries out the DPIA):

[ ]  Yes

[ ]  No

If the planned measures are not adequate to mitigate the risks associated with the processing activities, or if there are no measures that can be implemented to mitigate the risks, a prior consultation with the supervisory authority (in Finland the Finnish Data Protection Ombudsman) is required before initiating the processing of personal data. Contact Tampere University’s designated data protection officer for assistance with the prior consultation.

|  |
| --- |
| Data protection officer at Tampere UniversityEmail: dpo@tuni.fi |

1. This refers to the level of risk that remains after you have implemented the necessary protection measures. [↑](#footnote-ref-1)