Concise assessment of data protection risks in research

Guidelines
Tampere University
Data protection officer dpo@tuni.fi
February 2021
Assessment of data protection risks

• The risk assessment process is divided into the following stages:
  i. Concise risk assessment
  ii. Data protection impact assessment (DPIA)
  iii. Prior consultation with the supervisory authority

• i) A concise assessment of the risks associated with processing personal data must always be completed before processing personal data.

• ii) If the concise assessment reveals that the processing activities pose a high risk to data subjects, it is necessary to also carry out a data protection impact assessment (DPIA).

• iii) If the data controller does not take measures to mitigate the risks, a prior consultation with the supervisory authority must be arranged after completing the DPIA.
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 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?
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 category data* is data that reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic and biometric data when it is used for identification purposes, and data concerning health or data concerning an individual’s sex life or sexual orientation.

• Also: personal data relating to criminal convictions and offences or related security measures constitute special category data.
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;
The following slides are consistent with Tampere University's concise risk assessment template:
Elements of a concise risk assessment

• You must assess each processing activity against the following criteria:
  • the **risks** associated with the processing activity;
  • the **likelihood** of the risk (improbable possible, probable, almost certain);
  • the **severity** of the risk (serious harm, some impact, minimal impact);
  • the **measures** taken to mitigate the risk;
  • **remaining risk** = the level of risk that remains after you have implemented the necessary protection measures (low, medium or high risk).

• Assess the risks and consequences from the **perspective of your data subjects** (=research subjects).
# Elements of a concise risk assessment

<table>
<thead>
<tr>
<th>Severity of the breach or damage</th>
<th>Low risk</th>
<th>Moderate risk</th>
<th>High risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serious</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identified impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor impacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likelihood of the breach or damage</td>
<td>Remote</td>
<td>Possible</td>
<td>Highly likely</td>
</tr>
</tbody>
</table>
Risks

- A personal data breach can have serious consequences especially if it leads to the loss or unauthorised disclosure of personal data.
- The damages may be financial (such as fraud or identity theft), physical (such as violence or a threat thereof) or non-material (such as damage to reputation or loss of confidentiality of personal data).
- The level of risk depends on the likelihood and severity of the risk:
  - risk = severity of harm x probability of occurrence
Identifying data protection risks

• What risks are associated with the processing activities that you will perform at different stages of your research study? The processing of personal data means all processing activities involving personal data, such as collecting, storing, analysing, retaining, disclosing, archiving, deleting and destroying personal data.

• Assess the potential risks from the perspective of your data subjects.

• You can consider, for example, the following questions:
  • What types of processing activities will be carried out in the course of your research?
  • Who will process personal data at different stages of your research?
  • Where will you store personal data? In what format?
  • How and where will you transfer personal data at different stages of your research?
  • How extensively will personal data be processed? Will different categories of personal data be combined? Will you process special category data?

→ What are the risks associated with your processing activities?
Measures to mitigate risks

- The data controller must implement “appropriate technical and organisational measures to ensure a level of security appropriate to the risk”.
- Compliance with data protection principles is required by design and by default.
- Data protection risks can be controlled by taking a range of administrative and technical measures, such as
  - pseudonymisation of personal data
  - carefully determining the persons who are authorised to process personal data
  - carefully assigning user rights
  - storing personal data in encrypted form
    - such as username+password, encrypted hard drive, file encryption
  - encrypting personal data whilst it is being transferred:
    - such as access to a secure processing environment, encrypted email and attachments
- The risk assessment primarily focuses on the risks that remain after appropriate data protection measures have been put in place.
- Read more: Information security guidelines on the intranet
Documenting the risk assessment

• The risk assessment must be documented.
• There is no definitive template that you must follow when conducting your concise risk assessment. You can, for example, record the process in your data management plan, research plan, grant proposal, or request for an ethical review.
• You can also utilise Tampere University’s risk assessment form and enclose it with the rest of your project documents.
• The risk assessment template is available on the Data protection page on the University’s public website: https://www.tuni.fi/en/research/responsible-research/data-protection
Practical examples

• The following slides contain practical examples of processing activities and related risks.
• The examples highlight elements that may pose a risk to data subjects.
• The list of examples is not exhaustive but will help you identify potential risks to the rights and freedoms of your data subjects.
Example 1

A researcher interviews 20 vocational education teachers about their career paths. The researcher saves the data on his or her personal computer and sends the interviews to an external service provider for transcription.

• Points to consider when assessing risks:
  • What topics will be discussed during the interviews? Could the accidental disclosure of interview data to the interviewees’ employer cause harm to the interviewees?
  • Risks associated with data transfer: How will the data be transferred to the external service provider? Where will the service provider store the data?
  • Measures to reduce risks: pseudonymisation; storing data in a location recommended by Tampere University; password-protecting data; storing data in an encrypted form; file transfer encryption.
Example 2

Information about the family relations of Members of Parliament is collected from interviews published in magazines (n=25). The personal data will only be processed by a doctoral researcher and his or her supervisor.

- Points to consider when assessing risks:
  - The data includes special category data (political opinions) that the data subjects have brought into the public domain.
  - The data also includes their family members’ personal data.
  - Measures to reduce risks: careful planning of data transfer and storage.
Example 3

A research project collects health information from sexual minorities in five countries on three continents. Health data will be combined with information about the participants’ educational background and that of their ancestors going back for three generations. The project involves 2,500 research participants as well as personal data concerning their relatives’ educational background. The data will be saved on a shared platform, and the researchers will also store data on their office computers and home computers for analysis purposes.

• Points to consider when assessing risks:
  • Processing of special category data (sexual orientation, health data).
  • Data storage; sharing data with research groups?
  • Possible transfer of data outside of the European Economic Area?
  • Storing data on researchers’ home computers?
  • Measures to reduce risks: careful planning of data transfer and storage; informing researchers of the security of processing.
Example 4

• A research project will collect blood samples from 385,000 participants to analyse their genomes. Genome data will be combined with data about the participants’ lifestyle, education, taxable income and with information about where previous generations of their family lived.

• Points to consider when assessing risks:
  • Sensitive personal data will be extensively processed and combined during the project. Unauthorised disclosure of the data cold cause significant financial damage to the research participants.
Example 5

• Health data concerning 40,000 people will be collected during an international vaccine research project. At the beginning of the study, the participants will fill out an in-depth survey that includes detailed demographic questions (such as country, gender, age, ethnic group) and health questions. After receiving the studied vaccine, the participants will keep an online diary of any symptoms they experience in the two months following vaccination. During the study, two blood samples will be obtained from the participants and they will also self-collect nasal swap samples on a weekly basis and send them to the researchers. Information about the participants’ health will also be collected from existing records. The data will be analysed by researchers in five countries.

• Points to consider when assessing risks:
  • Special category data (health data, ethnic group) will be extensively collected during the project from the research participants and by combining collected data with data retrieved from different records.
  • What risks could the unauthorised disclosure of data pose to data subjects?
  • Data is stored both in paper form (initial survey, consent form) and electronic form (storing the survey in electronic form, the diary of symptoms).
  • Measures to reduce risks: careful planning of data transfer, data sharing and storage; informing researchers of the security of processing.
Example 6

• A longitudinal study examines the life of Sami children (30 families) in two municipalities in Finland with a large Sami population. The children are filmed in daycare centres and schools and during their free time. The research data contains interviews with the children, their teachers and their parents as well as documents concerning, for example, their grades.

• Points to consider when assessing risks:
  • The project involves the processing of special category data (ethnic minority; 30 families is quite a large sample considering the size of the ethnic group in question).
  • Safe storage of the data during the longitudinal study?
  • Measures to reduce risks: careful planning of data transfer and storage; informing researchers of the security of processing.
From a concise risk assessment to a data protection impact assessment (DPIA)

• When is it necessary to complete a DPIA?
  1. A DPIA is required if the concise risk assessment shows that the processing activities pose a high risk for data subjects.
  2. Specific processing activists that necessitate a DPIA are listed in the GDPR.
  3. Specific processing activities that necessitate a DPIA are identified by data protection authorities.
  4. When a DPIA is required by national law.

• Read a detailed description of the process: https://tietosuoja.fi/en/impact-assessments

• It will be easier and faster to carry out a DPIA if you have carefully completed the concise risk assessment.

• The DPIA template is available on the Data protection page on the University’s public website: https://www.tuni.fi/en/research/responsible-research/data-protection
Other data protection documentation

Remember also these:

• Privacy notice
• Data protection impact assessment (DPIA) (must be completed if the risk assessment reveals that processing poses a high risk for data subjects)
• Data processing agreements (if personal data will be processed, for example, outside of the research group)
• Joint controller agreement (in case of multiple data controllers)
Questions?

Contact: researchdata@tuni.fi