university of groningen

Data Protection Impact Assessment (DPIA)

Introduction and tips

Version: 10 October 2024

Privacy & Data Protection

Digital Competence Centre

university of groningen

Data Protection Impact Assessment (DPIA)

Introduction and tips

Are you going to start a project that involves processing personal (sensitive) data, and:

- you are not sure whether you need to do a DPIA or
- you are requested to do a DPIA?

Please read this document to learn about what a DPIA is, when you need to perform a DPIA, and what the process looks like!

Table of contents

university of groningen

What is a DPIA?

A Data Protection Impact Assessment is a method to build and demonstrate compliance with the GDPR. As the term already reveals, it is an assessment of how a project involving personal data might affect participants. The GDPR introduces the DPIA as a mandatory requirement for specific cases in which there is likely a high risk to the rights and freedoms of the research participants. The DPIA also aims to implement proper data protection measures during the project to eliminate or reduce the risks.

If you want to know more about DPIA please take a look at this short animated video.

Do you know that the Digital Competence Centre (DCC) may give you and your research team a short introduction to the DPIA method? Contact dcc@rug.nl.

When do I need to perform a DPIA?

A DPIA is necessary when research is likely to result in a high risk for the participants. But what does this mean?

A risk for a participant in the context of data protection involves a violation of their right to privacy with an impact on their daily lives. For example, if a participant admits company tax fraud during an interview, and this gets out then the participant may face being fired and prosecuted. The impact may have nothing to do with the data, but can be real-life material consequences of not taking the right precautions when designing the data processing.

Relevant criteria to determine if a DPIA is necessary

The European Data Protection Board and the Dutch Autoriteit Persoonsgegevens defined several legal criteria for when to conduct a DPIA. However, these lists are non-exhaustive and they are generally formulated and not specifically tailored to research. To provide extra guidance in determining whether a DPIA is necessary for a specific research project, the following criteria were developed at the University of Groningen:

1. Participants may be considered vulnerable

People may be regarded as vulnerable if they have difficulties understanding information or when the consequences of the research might impact them heavily. Think of children, elderly people, refugees, victims, patients, etc. Vulnerabilities are context dependent. Power imbalances or emotional involvement could also contribute to the level of vulnerability.

2. The data are sensitive

Using special categories of personal data or other sensitive data such as financial situation, criminal records, and location data can have a greater impact on people when these data are misused.

3. The research entails processing of data on a large scale

Risks can also increase when data processing becomes large-scale. The amount of data, the number of participants, the duration of the research project, and the geographical scale can all be reasons to perform a DPIA, such as the following examples:

- Personal data measured over a long period of time, such as longitudinal data or panel research, has a higher risk of potential harm to participants in case of a data breach, since a larger range of their data would be exposed.
- If more individuals join the participant pool (>1000 participants), a data breach could have a more significant impact on a greater number of people.
- If the research takes place on a global scale with participants from all over the world, it would count as large-scale.

4. Data from different sources are connected

Combining different data sets creates risks, such as an increased risks of re-identification. In addition, participants may not always expect that their data is enriched by data from other sources. This is especially an issue in secondary use of data.

5. Implementation of invasive technologies, or use of new technologies

A DPIA is necessary when we do not fully understand the consequences of data processings, and this is often the case with new or invasive technologies. Examples are: continuous monitoring of participants' lives or bodies, e.g. with a smartwatch and GPS; use of AI tooling; other new technological solutions which may bring uncertainties about which data is collected, how the data will be used and by whom (the UG or the manufacturer).

6. Involvement of different organizations or stakeholders

Involving many different organizations/other stakeholders in your research project is a risk-contributing factor. This is especially the case when parties in non-EU/EEA countries are involved, when dealing with parties with a low maturity level in data protection, and/or if the parties may have different aims regarding the use of data (e.g. commercial).

7. Difficulties exercising the rights of participants

A DPIA may be necessary when we can expect people to have difficulties exercising their rights as defined in the GDPR (See rights of the data subjects). E.g. in research that uses deception or covert observation, when research takes place in countries that do not have the same level of data protection as the EEA, or when research aims to influence/nudge people, fully informing the participants beforehand might not always be possible or desirable. These examples require careful assessment.

8. Research entails automated decision-making

The right to not be subject to automated decision-making applies when decision-making would affect someone's personal life (e.g. whether a person will get a loan based on a decision-making algorithm). Are you using automated decision-making that might impact someone's personal life? Then a Data Protection Impact Assessment (DPIA) is **mandatory**.

9. Other high risk to the rights and freedoms of your participants

All the points above do not constitute an exhaustive list. There might be other cases that could result in high risk for your participants. If you are unsure about a case, contact your faculty's Privacy & Security (P&S) coordinator or dcc@rug.nl.

university of groningen

How do I perform a DPIA?

The methodology adopted at the UG includes a multistakeholder approach. It provides a flexible, structured way to clarify internal responsibilities and document actions. In this document you can learn more about the process.

Initiation phase - Assessment of the need for a DPIA

If you think you need to do a DPIA or are requested to do so, please contact your faculty's P&S coordinator and discuss the case with them. Provide the P&S coordinator with the Research Data Management Plan (RDMP) and your project proposal, if you are already in possession of these documents. The P&S coordinator, a data steward and the legal department will discuss your case. They will advise you about the need to carry out a DPIA or data protection measures you can apply to mitigate the risks.

TIP #1: Preparing the RDMP is an excellent way to start thinking: What kind of data will I need? Am I collecting personal or sensitive data? Do I need to ask for consent? Am I re-using personal data from other projects? Am I allowed to do that? How can I protect the privacy of the people involved?

Do you need help with the RDMP? Contact the Data Steward of your faculty or the DCC (dcc@rug.nl).

Execution phase - Risk analysis and mitigation measures

Based on the information collected in the preparation phase, the DPIA team will analyze the possible risks and define data protection measures to mitigate them. All the results will be documented in a report. The report will be shared with the legal department, including the Data Protection Officer, for evaluation.

The Dean of your faculty will be informed about the results of the DPIA. As a researcher, you are responsible for implementing the measures during the project. The P&S coordinator will help you if you need to prepare agreements with third parties.

If the DPIA was requested by the founder of the project or by the Ethics Committees (or Institutional Review Board) of your faculty, the P&S coordinator of your faculty will provide them with the final report.

TIP #2: Make sure to involve your team in the DPIA. Are you a PhD? Discuss the participation of the DPIA with your supervisor. Do you have a data manager or a PhD in your project? Involve them in the DPIA. This will support them in designing their tasks and learn about privacy and data protection.

Implementation phase - Implementation of the measures

After the execution phase is finished, and the data protection measures have been designed and implemented in your research, you can start your research. Remember: as a researcher/project leader, you are responsible for implementing and executing the measures during your project. If you encounter any problems, report to the P&S coordinator.

university of groningen

TIP #3: If you collaborate with external organizations in your project, a DPIA is an excellent way to clarify responsibilities. The P&S coordinator can help you if you need any agreement.

Sustainability phase - Monitoring of changes and definition of adjustments.

If any changes or deviations occurred during your project, you might need to re-evaluate the DPIA report. Depending on the size of the deviations or changes, potentially repeat phases 2 (execution) to 4 (sustainability). Please consult with the P&S coordinator, they will help you analyze the case and define the necessary adjustments.

TIP #4: Your ethics and legal dilemmas can be interesting and enrich your research community! Did you think of sharing your experience with your colleagues? Take a look at this example on "How the GDPR can contribute to improving geographical research".

Do you want to know more about data protection? Consult the DCC website section on Privacy & Data Protection.