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 your responsibility, the DPIA process and who can help you!

What is a DPIA?

The GDPR introduces the DPIA as a mandated assessment for specific cases in which there is a high risk to the rights and freedoms of the research participants. The DPIA process aims to identify the privacy and data protection risks and implement proper measures during the project to eliminate or reduce them. If you want to know more about DPIA please take a look at this short animation.

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.

How do I perform a DPIA?

A Data Protection Impact Assessment is a method to build and demonstrate compliance with the GDPR. 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 - This phase aims to clarify whether a DPIA is necessary.

If you think you need to do a DPIA or are requested to do so, please contact your faculty's Privacy & Security (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.

P&S coordinator, a consultant of the DCC and the legal department will discuss your case. They will advise you about the need to carry out a DPIA or measures you can apply to mitigate the risks.

Your one-stop for research IT and data

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 DCC (dcc@rug.nl).

Preparation phase- This phase aims to collect all the information needed to describe the intended data process and to plan the next phase.

If you have to do a DPIA, a team of experts will be defined and this team will execute the risk analysis with you. The team will design some measures to mitigate the risks. You must implement these measures during the project.

As an expert on your research subject, you will contribute to the DPIA by providing information about the research method, procedure and good practices applied in your field of research.

TIP #2: draw the data flow of the intended processes. It is an excellent way to identify the possible risks in your project. Do you know that the DCC can help you design the data flow?

Execution phase - Based on the information collected in the preparation phase, the DPIA team conducts the risk analysis and defines measures to mitigate the risks.

The DPIA team will analyze with you the possible risks and define 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 legal department will help you if you need to prepare agreements with third parties (abjz@rug.nl).

If the DPIA was requested by the founder of the project or by the Ethics Committees (or Institutional Review Board) of your faculty, you could provide them with the final report.

TIP #3: Be 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. They will start designing their tasks and learn about privacy and data protection.

Implementation phase - This phase aims to implement the measures.

As a researcher/project leader, you are responsible for implementing the measures during your project. If you encounter any problems, report to the P&S coordinator.

TIP #4: If you collaborate with external organizations in your project, the DPIA is an excellent way to clarify responsibilities. The legal department can help you if you need any agreement.

Sustainability phase - This phase includes the monitoring of the implementation phase, the identification of deviations or changes and the definition of adjustments. Depending on the size of deviations or changes potentially repeat phases II to IV.

If any changes or deviations occurred during your project, you might want to re-evaluate the DPIA report.

Please consult the P&S coordinator they will help you analyze the case.

TIP #5: The GDPR defined some exemptions for research. Do you want to learn more about what these exemptions entail? The DCC can help you.

TIP #6: 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.

Do you want to know more about data protection?

Consult Privacy & Data Protection.