

Conducting the Data Privacy Impact Assessment (DPIA)

Planning a project involving the processing or collection of personal data? Conduct the DPIA before moving forward. It helps you identify and mitigate data privacy risks.

1. Identify why collecting and processing data is required and the strictly necessary data points



2. Identify the data flow and review the IT environment, access, storage, and data transfer. In case of cross border data transfer, a Data Transfer Impact Assessment may be required



3. Identify the regulatory framework and to what extent privacy by design and default must and can be implemented



4. Rate the risks as “high”, “medium” or “low”, and identify and document 1st-line-appropriate controls



5. If the risks remain high despite any planned mitigating measures, a consultation with the competent Data Protection Authority may be necessary depending on the jurisdiction



Where do I conduct the DPIA?

The Pre-DPIA and DPIA should be conducted via the OneTrust tool. If OneTrust is not available in your Business Unit, please approach your local Data Protection Officer (DPO) or Data Protection & Privacy Contact (DPPC) for a respective template.



Preliminary Step: Conduct a Pre-DPIA

The Pre-DPIA helps assess if your project intends to process personal data and the scope of the processing itself. Depending on the jurisdiction, the size and nature of the project, and the type of data to be processed, a full DPIA may be necessary.

