

Data Protection Impact Assessment (DPIA) Procedure

Reference GDPR DOC 1.3.5

DocumentKits issue no 1.1

DocumentKits issue date 24 November 2022

1. Scope

All projects that involve high-risk personal data processing or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a data protection impact assessment (DPIA).

DPIAs and screening questions are performed using the [Data Protection Impact Assessment \(DPIA\) Tool](#).

2. Roles and responsibilities

2.1 The [select role] is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.

2.2 <<Content removed for sample purposes>>

2.3 <<Content removed for sample purposes>>

Procedure

3.1 The [select role] identifies the need for a DPIA at the start of each project before [Organisation Name] starts processing personal data, assessing the project and type of personal data involved, or processing activity, against the screening questions set out in the [Data Protection Impact Assessment \(DPIA\) Tool](#).

3.2 A stage 1 DPIA (screening questions) is completed for all projects involving the processing of personal data.

3.3 <<Content removed for sample purposes>>

4. Identify privacy risks

4.1 [Organisation Name] assesses the privacy risks for each processing activity as described above by:

4.1.1 <<Content removed for sample purposes>>

4.1.2 Using the likelihood criteria in the [Data Protection Impact Assessment \(DPIA\) Tool](#) (1 – low, 2 – medium and 3 – high) to indicate the likelihood of the risk occurring;

4.1.3 <<Content removed for sample purposes>>

4.1.4 <<Content removed for sample purposes>>

4.2 <<Content removed for sample purposes>>

4.2.1 <<Content removed for sample purposes>>

4.3 [Organisation Name] identifies solutions to privacy risks, assigns a risk treatment owner and sets a target date for completion. These are recorded in the [Risk Treatment Plan](#) alongside the output of the [Risk Management Procedure](#).

4.4 <<Content removed for sample purposes>>

5. Prior consultation

5.1 When the DPIA identifies that processing of personal data will result in high risk to the data subject in the absence of risk mitigating measures and controls, [Organisation Name] consults with the Information Commissioner's Office and/or supervisory authority as follows.

5.2 When [Organisation Name] requests consultation, it provides the following information:

5.2.1 <<Content removed for sample purposes>>

5.2.2 <<Content removed for sample purposes>>

5.2.3 <<Content removed for sample purposes>>

5.2.4 <<Content removed for sample purposes>>

5.2.5 A copy of the DPIA.

5.2.6 Any other information requested by the supervisory authority.

Document owner and approval

The [select role] is the owner of this document and is responsible for ensuring that it is kept up to date.

The current version of this document is available to [Specify which members of staff this document is intended for] and is published [Describe the location(s) – electronic and physical – where this document is available].

Its approval status can be viewed in the [Master List of Document Approval](#).

IT Governance Ltd



Our expertise,
your peace of mind

This document contains material that is distributed under licence from IT Governance Ltd.