

Privacy by Design Procedure

Reference GDPR DOC 1.3.2

DocumentKits issue no 1.1

DocumentKits issue date 25 November 2022

1. Scope

This procedure applies to [Organisation Name] and all those working under its control (permanent and temporary employees, contractors and workers). It applies to all new and amended personal data processing activities that [Organisation Name] develops.

<<Content removed for sample purposes>>

2. Roles and responsibilities

2.1 Process Owners are responsible for developing the design document and test plan, amending them in response to the data protection impact assessment (DPIA) (as necessary), and overseeing the testing.

2.2 <<Content removed for sample purposes>>

2.3 <<Content removed for sample purposes>>

3. Procedure

All new personal data processing activities and changes to such activities are documented. [If you use a standard template for design, link to it here, or describe the format and general expectations of the design document.]

3.2 All designs must include the following information:

3.2.1 A defined purpose for the processing.

3.2.2 <<Content removed for sample purposes>>

3.2.2.1 <<Content removed for sample purposes>>

3.2.2.2 Where legitimate interest is the lawful basis, the Process Owner must

conduct a legitimate interests assessment using the [Legitimate Interests Assessment Tool](#).

3.2.2.3 <<Content removed for sample purposes>>

3.2.3 A clear statement of the minimum personal data needed to achieve the purposes.

3.2.4 Measures that will be applied to secure the confidentiality and integrity of the personal data.

3.2.5 <<Content removed for sample purposes>>

3.2.6 <<Content removed for sample purposes>>

3.2.7 <<Content removed for sample purposes>>

3.2.8 <<Content removed for sample purposes>>

3.3 The design document is accompanied by a test plan which must set out how [Organisation Name] will confirm that the processing activity conforms to the design.

3.4 All new personal data processing activities and changes to such activities that present a high risk to data subjects are subject to DPIA, as set out in the [Data Protection Impact Assessment Procedure](#).

3.4.1 <<Content removed for sample purposes>>

3.4.2 Where [the Information Commissioner's Office or other supervisory authority] consultation is required, [Organisation Name] ensures this process is complete before proceeding with the processing.

3.4.3 <<Content removed for sample purposes>>

3.5 Where the processing activity is electronic, [Organisation Name] follows defined secure coding practices.

3.6 <<Content removed for sample purposes>>

3.6.1 <<Content removed for sample purposes>>

3.7 All new processing activities are added to the [Record of Processing Activities](#).

3.8 Amended processing activities are updated in the [Record of Processing Activities](#) as necessary.

3.9 Data subjects affected by new/amended processing activities are notified in accordance with the [Privacy Notice Procedure](#) and [Communications Procedure](#).

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