Privacy by Design Procedure

Reference: GDPR DOC 1.3.2
DocumentKits Issue No: 1.0
DocumentKits Issue Date: 01/03/2022

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.

A processing activity is any function applied to personal data, including collection, storage, encryption, transmission, etc.

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 The
"Data Protection Officer/GDPR Owner"

is responsible for reviewing processing activities and the outcome of this procedure to ensure that personal data processing meets the GDPR's data processing principles.

2.3 <<Content removed for sample purposes>>

3. Procedure

3.1 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 The lawful basis for the processing.
3.2.2.1 Where consent is the lawful basis, the design should align with the
"Data Subject Consent Procedure."ACCEPT TEXT

SAMPLE

3.2.2.2 <<Content removed for sample purposes>>
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."ACCEPT TEXT

3.4.1 'High risk to data subjects' is "describe how the organisation determines this."

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

3.4.3 The design document and test plan are updated as necessary in response to the DPIA and consultation.

3.5 Where the processing activity is electronic, Organisation Name follows defined "secure coding practices."ACCEPT TEXT

3.6 The processing activity is tested in accordance with the test plan referred to in 3.3 before it is released.
3.6.1 Organisation Name uses "randomly generated/artificial personal data" to test processing activities.

3.7 <<Content removed for sample purposes>>

SAMPLE

3.8 <<Content removed for sample purposes>>

3.9 <<Content removed for sample purposes>>

Document owner and approval

The
"Data Protection Officer/GDPR Owner"

is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.
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.

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

SAMPLE