Data Protection Impact Assessment Procedure

Reference: GDPR DOC 2.4
DocumentKits Issue No: 1.0
Organisation Issue No:
DocumentKits Issue Date: 15/11/2019
Organisation Issue Date:

1. Scope

All projects that involve processing personal data, 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).

2. Responsibilities

2.1 The Data Protection Officer / GDPR Owner is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.

2.2 Head of Risk and Data Protection Officer / GDPR Owner are responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

2.3 Risk owners are responsible for implementing any privacy risk solutions identified.

3. Procedure

3.1 The Data Protection Officer / GDPR Owner / project manager / programme office identifies the need for a DPIA at the start of each project, 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 Using the criteria below, following the likelihood and impact matrix, Organisation Name defines the risks to rights and freedoms of data subjects as (Data Protection Impact Assessment (DPIA) Tool):

Likelihood and impact matrix

Likelihood	**3**	0	3	6	9
	2	0	2	4	6
	1	0	1	2	3
		0	**1**	**2**	**3**
					Impact

Risks to rights and freedoms of data subjects:

Risk Level	From	To	GDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

4. Data processing workbook (data flow)

4.1 Organisation Name records key information about all personal data processed for each project in the DPIA Tool workbook (Data Protection Impact Assessment (DPIA) Tool). This includes a description of the processing and purposes; legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects (as per the matrix and risk level definitions in clause 3.2 above).

4.2 Organisation Name captures the type of processing activity associated with the personal data being processed as part of the project in the DPIA Tool workbook (Data Protection Impact Assessment (DPIA) Tool). These are categorised as:

- Collection
- Transmission
- Storage
- Access
- Deletion

4.3 Organisation Name establishes on what lawful basis the data is being processed and its appropriate retention period (in line with Retention of Records Procedure).

4.4 Organisation Name identifies the category of data processed, whether it is personal, special or that of a child's, and the format of the data.

4.5 Organisation Name identifies who has access to the data (individuals, teams, third-parties or data processor) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place and / or if it is transborder processing.

5. Identify privacy risks

<< 5.1 – 5.5 removed for sample purposes >>

6. Prior consultation (Article 36, GDPR)

6.1 Where 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 supervisory authority
"at this location"

using the following method.

6.2 When Organisation Name requests consultation from the supervisory authority it provides the following information:

6.2.1 detail of the responsibilities of Organisation Name
"controller/processor/joint controller"

and the
"data controller/processor/joint controller"

involved in the processing;

6.2.2 purpose of the intended processing;
6.2.3 detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s);
6.2.4 contact details of the Data Protection Officer / GDPR Owner as recorded
"where"

6.2.5 a copy of the data protection impact assessment; and

6.2.6 any other information requested by the supervisory authority.

Document Owner and Approval

The Data Protection Officer / GDPR Owner is the owner of this document and is responsible for keeping it 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 Master List of Document Approval.