

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE (TIER 2)

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

Document History

#	Version	Date	Created/ Modified by	Change Doc. No & Brief description of the change incorporated	Approved by / Approved Date
1	1.0	24 th July 2021	Zamir Shaikh	Initial Version	Azim Shaikh

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE (TIER 2)

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 is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.
- 2.2 Data Protection Officer 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 Owner] s is responsible for implementing any privacy risk solutions identified.

3. Procedure

- 3.1 The Data Protection Officer / Management Committee 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 DPIA tool ([GDPR REC 4.4](#)).
- 3.2 Using the criteria below, following the likelihood and impact matrix, MBP'S defines the risks to rights and freedoms of data subjects as (GDPR REC 4.4):

Likelihood and impact matrix (see next page):

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE (TIER 2)

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 MBP'S records key information about all personal data processed for each project in the DPIA Tool workbook (GDPR REC 4.4). This includes a description of the processing and purposes; legitimate interests pursued by the processor; 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 MBP'S captures the type of processing activity associated with the personal data being processed as part of the project in the DPIA Tool workbook (GDPR REC 4.4). These are categorised as:
- Collection
 - Transmission
 - Storage
 - Access
 - Deletion
- 4.3 MBP'S establishes on what lawful basis the data is being processed and its appropriate retention period (in line with Retention of Records Procedure GDPR DOC 2.3).
- 4.4 MBP'S identifies the category of data processed, whether it is personal, special or that of a child's, and the format of the data.

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE (TIER 2)

- 4.5 MBP'S 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 MBP'S assesses the privacy risks for each process activity as described in clause 3 above by:
- 5.1.1 Identifying and describing the privacy risk associated to that process activity
 - 5.1.2 Using the likelihood criteria (1 – low, 2 – medium and 3 - high), scoring the likelihood of the risk occurring
 - 5.1.3 Using the impact criteria (0 – zero impact, 1 – low, 2 – medium and 3 - high) of the risk should it occur
 - 5.1.4 Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects.
- 5.2 In assessing the privacy risks, MBP'S considers: risks to the rights and freedoms of natural persons resulting from the processing of personal data; risks to the business (including reputational damage); and its objectives and obligations (both regulatory and contractual).
- 5.3 MBP'S identifies solutions to privacy risks, assigns a risk treatment owner and sets a target date for completion.
- 5.4 MBP'S prioritises analysed risks for risk treatment based on the risk level criteria established in clause 3.2 above.
- 5.5 MBP'S risk owner, in consultation with Data Protection Officer, approves and signs off each DPIA for each data processing activity.

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, MBP'S consults with the supervisory authority at Pune office, using the following method.
- 6.2 When MBP'S requests consultation from the supervisory authority it provides the following information:
- 6.2.1 detail of the responsibilities of MBP'S processor, and the data processor 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);

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE (TIER 2)

- 6.2.4 contact details of the Data Protection Officer as recorded in the contract agreement
- 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 Approver

The Data Protection Officer is the owner of this document and is responsible for ensuring this procedure is reviewed.

A current version of this document is available to all/specified members of staff on the company intranet.

This procedure was approved by Board of Directors and is issued on a version controlled basis under his/her signature