Data Protection Impact Assessment (DPIA)

Form No: QMS 32	Revision No: 01	Date of Issue: 22 October 2018

Section 34(1) of the Data Protection Act (DPA) 2017 stipulates that all controllers and processors must carry out a DPIA prior to the processing of personal data where such processing is likely to present high risk to individuals. A DPIA helps to identify privacy risks, foresee problems and bring forward solutions. It serves as an assessment tool to decide whether the security measures in place are adequate compared to the risks to individuals and whether the necessity of an envisaged processing operation does not outweigh the rights and freedoms of individuals.

The Data Protection Office has issued this template for guidance purpose only and is subject to future updates, if required. You are also advised to consult the document on '*High risk processing operations'* and '*Guide on how to complete the Data Protection Impact Assessment Form*' available on the website of the Data Protection Office.

Step 1: General Information

1.1 Name of controller/processor *(delete as appropriate)*
1.2 Address
1.3 Telephone Number
1.4 Name of contact person
1.5 Is the controller/processor registered with the Data Protection Office?
1.6 Have you designated an officer responsible for data protection compliance issues?
1.7 Are you certified ISO/IEC 27701 Privacy Information Management System?

Step 2: Details of project/envisaged processing

2.1 Description of project/processing
2.2 Purpose/s of project/processing
2.3 How do you plan to prevent function creep, i.e., preventing the processing of personal data beyond the original context of use?
2.4 Benefit/s of project/processing

2.5 Type/s of processing involved
2.6 Reason/s for doing a DPIA
2.7 Categories of data subjects whose personal data will be processed

Step 3: Details of processing

Nature of the processing

3.1 List the types of data which will be processed
3.2 (a) Will the processing involve special category/ies of personal data? **(b) If yes,** **(i) List all the special category/ies of personal data that will be involved.** **(ii) Specify under which condition/s of section 29(1) of the DPA will it/they be processed?**
3.3 (a) Will the processing involve personal data of children below the age of 16 years? **(b) If yes,** **(i)How do you plan to obtain the consent of their parent or guardian?** **(ii) How do you plan to verify that consent has been given or authorised by the holder of parental responsibility?**
3.4 What is the source of personal data?
3.5 In the event that data will be collected directly from individuals, do you plan to inform them of the prescribed list of information defined under section 23(2) of the DPA at the time of collection?
3.6 In the event that data will not be collected directly from individuals, how do you plan to inform them of the prescribed list of information defined under section 23(4) of the DPA?
3.7 Describe how data will be collected, used, stored and deleted? (Note: You may use Data Flow Diagrams to illustrate same.)
3.8 In what format/s will personal data be collected and stored?

3.9 Describe any transfer method (internally and externally) of personal data involved in the processing?
3.10 What geographical location/s will be involved during the processing?
3.11 Who will be accountable for the processing of data?
3.12 Who will have access to the personal data?
3.13 List all the stakeholders involved in the processing with their respective roles?
3.14 (a) Do you plan to use the services of a processor during the envisaged processing? **(b) If so,** **(i) How will the controller ensure that the processor/s comply with the instructions of the controller?** **(ii) How do you plan to notify the processor holding the data for destruction of the data when the purpose of processing lapses?**
3.15 Will the data be shared to any third party? If so, for which purpose/s?
3.16 Will the disclosure of personal information be considered lawful under the Data Protection Act or other laws?
3.17 Describe the data security and organisational measures that will be implemented to protect data during the processing?
3.18 Do you plan any special security measures to prevent any potential data breach? If so, list them.
3.19 In case of personal data breach/es, **(a) How do you plan to notify the Data Protection Office?** **(b) How do you plan to communicate the data breach/es to any affected individual/s if it is likely to present high risks to him/her?**
3.20 Do you plan any audit/monitoring exercise to evaluate the effectiveness of technical and organisational measures for the envisaged processing?
3.21 Will data be encrypted and /or pseudonymised during the processing?
3.22 Will there be a disaster recovery plan to restore availability and access to personal data during physical/technical incidents?

3.23 Any other information regarding the nature of processing?

Scope of the processing

3.24 How many individuals' data will be processed?
3.25 What are the boundaries of the envisaged processing?
3.26 How often will the processing be carried out?
3.27 How long do you plan to keep the data?
3.28 Do you plan to delete or anonymise data as soon as the purpose of processing lapses?
3.29 (a) Will there be any transfer of personal data abroad? **(b) If yes, list the countries?** **(c) How do you plan to seek authorisation from the Data Protection Office for data transfers abroad in the event where you cannot provide proof of appropriate safeguards with respect to the protection of the personal data, or cannot rely on any of the exceptions provided in section 36(1) of the DPA?**
3.30 Any other information regarding the scope of processing?

Context of the processing

3.31 What procedures do you plan to have in place to handle requests from individuals regarding their rights to: **(a) Access their data?** **(b) Have their data rectified in case the data processed is inaccurate?** **(c) Erase their data as appropriate under section 39(2) of the DPA?** **(d) Temporarily restrict processing of their data as appropriate?** **(e) Object to processing of their data as appropriate?** **(f) Not be subject to decisions based solely on automated processing, including profiling, that have legal effects or that significantly affect them?**
3.32 How do you plan to inform individuals about their rights on the envisaged processing?
3.33 How far do you consider yourself meeting the expectations of individuals that their personal data will be processed in this manner?

3.34 If the processing entail potential risks to individuals, how do you plan to inform the latter to avoid any unforeseeable negative effects on them?
3.35 What is the current state of technological development/s available for the envisaged processing?
3. 36 Is there any preceding concern/s or apprehension/s with respect to this type of processing?
3.37 Is there any data protection issue/s which may affect the public regarding the envisaged processing?
3.38 How do you intend to seek the views of data subjects on the intended processing? Please provide your justifications.
3.39 Are employees trained for the envisaged processing?
3.40 How do you plan to include the envisaged processing in your record of processing operations carried out by the organisation?
3.41 Any other information regarding the context of processing?

Step 4: Necessity and proportionality of processing

4.1 What is/are your legitimate interest/s for the processing?
4.2 What is/are the lawful ground/s for the processing?
4.3 In the event that you will rely on consent of individuals as your lawful ground to process their data, **(a) Will the consent be considered valid, i.e., freely given, specific, informed and unambiguous?** **(b) How will you keep proof of consent?** **(c) What procedures will you keep to handle withdrawal of consent of individuals?** **(d) How will you verify that the consent requested is necessary and directly related to the performance of a contract or service related to the project/processing?**
4.4 How is the processing demonstrably necessary to meet the specific need/s?
4.5 How is the processing likely to be effective in meeting that need?
4.6 Are there alternative means for achieving the same outcome?

4.7 How will you ensure that data collected or processed is adequate, relevant and not excessive?
4.8 How will you ensure that data is accurate and up to date during the processing?
4.9 How will confidentiality, integrity, availability and resilience of data be ensured during the processing?
4.10 Will any loss of privacy be proportionate to the benefit/s gained?
4.11 How do you plan to provide any additional measures to support the rights of individuals during the processing?

Step 5: Risks Assessment

Risk No.	**Description /Nature of Risks**	**Likelihood of damage/ harm** • **Frequent** • **Occasional** • **Unlikely**	**Severity of damage/ harm** • **Critical** • **Moderate** • **Insignificant**	**Overall Risks** • **High** • **Medium** • **Low**

Step 6: Measures to mitigate risks

Note: Appropriate technical and organisational measures must be implemented to mitigate risks classified with overall risks of 'High' and 'Medium' in step 5.

Risk No.	**Measures to mitigate risks**	**Effect of Measures on risks** • **Eliminated** • **Reduced**	**Residual Effect** • **High** • **Medium** • **Low**

Step 7: Documentation

DPIA carried out by:			
Name of officer/s	**Designation of officer/s**	**Signature**	**Date**

DPIA reviewed by:			
Name of officer/s	**Designation of officer/s**	**Signature**	**Date**

DPIA approved by:			
Name of officer/s	**Designation of officer/s**	**Signature**	**Date**

Submission of a copy of DPIA to Data Protection Office: (In accordance with section 35(5) of the DPA)			
Name of officer	**Designation of officer**	**Signature**	**Date**