HOW TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT (DPIA)

What is a DPIA?

- A Data Protection Impact Assessment is a documented process whereby a Controller can identify the risks to personal data that may be caused by implementing a particular process, operation, or service that processes that personal data
- Through the identification of these risks, DPIAs support Controllers in deciding on steps to take to mitigate these risks

When is a DPIA required?

Controllers must carry out a DPIA before performing any data processing that is likely to result in a high risk to the rights of individuals, for example:

- When setting up initiatives involving the use of special categories of personal data
- When introducing novel methods for processing personal data (i.e. AI, algorithms, automation)
- When significant changes occur in an IT/information system involving personal data processing

Why are DPIAs necessary?

- DPIAs support Controllers in monitoring and addressing risks to data protection and individuals' rights
- DPIAs assist in the evaluation of a Controller's existing measures ecosystem against applicable protection regulations

In certain cases you may be required to notify the Office of Data Protection if the residual risk to the rights and freedoms of individual remain high.

Steps To Perform Data Protection Impact Assessment

Below are high-level steps organizations should take to perform a Data Protection Impact Assessment:

Identify

- Identify the activity, project, initiative, or process that will involve the processing of personal data

Evaluate

- Evaluate whether the identified activity, project, initiative or process requires a DPIA. Liaise with your organization's Data Protection Officer.
- Initiate a DPIA if any of the following applies:
  - Processing that is likely to result in a high risk to the rights of individuals
  - Processing involves novel or new technologies such as AI, machine learning, automated decision making and profiling
  - Processing of Special Categories of Data

Develop

- Develop a DPIA questionnaire that collects the following:
  - Description of the nature, scope, context, and purpose of the Processing
  - Assessment of the necessity, proportionality, and compliance measures
  - Identification and assessment of risks to individuals

Prepare

- Prepare a DPIA report for key stakeholders by consolidating the findings and actions from the questionnaire. The report should include the following:
  - Description of risk
  - Date identified
  - Risk Owner
  - Action / Risk Treatment
  - Timeline
  - Status

Follow-up

- Follow-up on the agreed Actions / Risk Treatment
- Ensure ongoing monitoring and review changes to the activity. Any substantive changes must undergo another evaluation.

DPIAs can be performed using specialized data privacy applications or via spreadsheet/word processing software. ADGM ODP provides sample templates for conducting DPIAs on the website as part of the guidance related to the ADGM Data Protection Regulations 2021.