NICCOM LLP
BARRISTERS & SOLICITORS

Privacy and Data Protection Snapshot Series

Data Protection Impact Assessment

A data protection impact assessment ("DPIA") is an ***evaluation*** of a project, process, or activity (PPA) within a data controller's operations, with a view to identifying the impact of the PPA on the personal data of data subjects. DPIAs are usually undertaken when a data controller intends to roll out a new PPA, or to modify existing ones, that may involve the processing of personal data.

A myriad of organisational activities can necessitate the conduct of a DPIA. For instance, an investment company rolling out a new mobile app for its customers, a medium-scale business changing its accounting software, a law firm updating its client filing from manual-based to electronic, an oil company outsourcing its HR function, etc., would all qualify as activities requiring a DPIA to be undertaken.

The main purpose of a DPIA is to ***gauge*** the *likelihood* that the PPA might breach the rights of some data subjects, as well as the *extent and impact* of such breach should it occur. It is usually undertaken as a pre-emptive step, akin to a risk assessment.

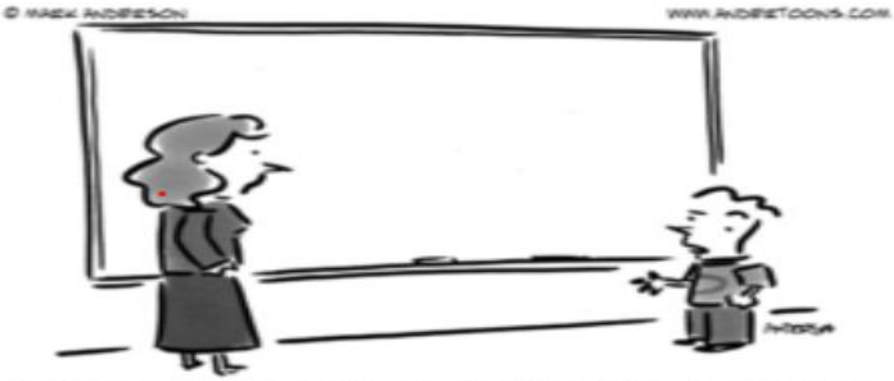
It is not mandatory for a data controller to perform a DPIA on all existing, new or modified PPAs. Pursuant to the NDPR Draft Implementation Framework issued by NITDA, a DPIA is required where a data controller intends on embark on a project "that is likely to result in significant risks to the rights and freedoms" of data subjects. Article 35 the GDPR adopted the word *high* in place of *significant*, but the import of its provision is similar to the provision in the NDPR Framework.

What type of projects would qualify as significant or high-risk, in the context of conducting a DPIA? Neither the NDPR Framework nor the GDPR expressly defined *significant* or *high-risk* projects. However, the GDPR suggested processing activities that may indicate that the anticipated processing is high-risk. Such activities include:

- Activities that may involve significant economic disadvantage, such as identity theft or fraud;
- Activities that may involve social disadvantage, such as discrimination;
- Activities that may place physical restrictions on data subjects;
- Activities that may limit/ prevent data subjects from exercising control over their data; and
- Activities that may involve sensitive information about data subjects being revealed or evaluated.[1]

The NDPR Framework also requires data controllers to have a DPIA policy to regulate the conduct of DPIAs within their operations. This can be a standalone policy or part of the privacy or security policy of the data controller.

[1] A list of criteria – endorsed by the European Data Protection Board (EDPB) – has been published to help organisations in determining whether a processing activity is likely to be considered a high risk.



Data controllers typically engage experienced privacy and data protection practitioners to conduct DPIAs. In Nigeria, only licensed data protection compliance organisations (DPCOs) are permitted to conduct DPIAs, where the data controller chooses to outsource same. The DPIA is expected to identify possible risk areas where data breaches may occur, and devise means of addressing the risk. Key areas to be covered during a typical DPIA include:

- The nature of activities being undertaken;
- How those activities involve and process personal data;
- The type of personal data being processed;
- The type of data subjects impacted;
- The nature of the risk to data subjects;
- The exact cause(s) of the risk to data subjects;
- The scope of processing (such as the categories and volume of data involved);
- Any relevant context (relationship with the data subjects, the current state of any technology used, etc.); and
- Finally, an assessment of the "necessity and proportionality" of the processing against the "purpose" of processing.

Data controllers are also required to conduct DPIAs on their existing processes, services and technology periodically to ensure continuous compliance. It is ultimately the data controller's responsibility to evaluate any proposed processing activities and determine whether a DPIA is required. In addition, it is leading practice to conduct a DPIA for all PPAs, whether the processing activity involved presents a significant risk or not.

A report is typically prepared at the end of a DPIA, documenting the relevant aspects of the DPIA, including the identified risks and the proposed treatment of such risks. It is also important to document the decisions made for all activities considered during the DPIA, regardless of whether the

DPIA was ultimately conducted. A record of all identified risks – even those that are not significant enough to require a DPIA – should also be maintained, so that those risks can be monitored along with other risks faced by the data controller.

On a final note, the importance of documentation cannot be overemphasized. Documented evidence is required even when there is a decision by the data controller not to go ahead with the DPIA or share the results of the evaluation. There may be a need, for the sake of transparency or consultation, to provide evidence of compliance in the event of an investigation by the supervisory authority, or where a data breach suit is filed by an aggrieved data subject.

NICCOM LLP is a licensed Data Protection Compliance Organisation (DPCO), and can provide data protection compliance services, as well as other related services required by data controllers. As a law firm, we are positioned to proffer legal advice on the impact of the NDPR to your organisation, and suggest recommendations on process improvement, where necessary.