

Data Protection

30th June 2025



Maryam Abdulsalam

The Importance of Data Protection Impact Assessment (DPIA) in an Organization[1]

Introduction

Effective protection of personal data is an essential objective in an organization. Data Protection legislations are enacted to ensure that deliberate efforts are being made by organizations, individuals, and entities to safeguard personal data, implement data protection best practices, and prevent potential breaches. An important obligation imposed on organizations by data protection legislations is the requirement to conduct a Data Protection Impact Assessment (DPIA) in various circumstances. This article examines the concept of a DPIA, the circumstances that require conducting a DPIA, the mode and implementation of DPIA, and its significance to organizations.

The Concept of Data Protection Impact Assessment (DPIA)

A DPIA is a process and systematic approach created to highlight and address potential privacy risks that might emerge during any data processing activity or proposed project impacting on privacy rights.

The Nigeria Data Protection Act (NDPA)[2] defines a DPIA as a systematic process and an assessment to identify the risks and impact of an envisaged processing of personal data in an organization. It is an assessment of the risks to the rights and freedoms of a data subject and the

---

[1] **Maryam Abdulsalam, Associate, Intellectual Property Department, SPA Ajibade & Co. Lagos, Nigeria.**

[2] Section 28 of the *Nigerian Data Protection Act* (NDPA) 2023.

measures targeted at addressing the risks, safeguards, security measures, and mechanisms to ensure the protection of personal data, taking into account the rights and legitimate interests of a data subject and other persons concerned.[3]

In the course of processing personal data or prior to the commencement of a project that would likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purposes, an organization is required to conduct a DPIA. The DPIA conducted should identify potential areas where breaches may occur and devise a means of addressing such risks.

DPIA foresees and anticipates potential risks and data breaches in an organization. DPIA is a proactive rather than a reactive process. It scrutinises the data processing activities and evaluates critical measures to be undertaken by an organization prior to implementation.[4]

The DPIA evaluates the source and types of personal data collected by an organization, the technical and organizational measures in place to store and protect the data, the volume, variety, and sensitivity of the data, the potential risks involved in processing, and the likely outcomes of the processing activities.

Instances in which a DPIA should be Conducted in an Organization

In Nigeria, pursuant to the provisions of the NDPA, the Nigeria Data Protection Commission (NDPC) recently issued the *NDPA-General Application and Implementation Directives* (GAID) 2025.[5] The GAID highlights the various circumstances in which organizations are mandated to conduct a DPIA. A DPIA is mandatory and shall be filed with the Commission in any of the following circumstances:[6]

a. When evaluation or scoring (profiling) data subjects;
b. When engaging in automated decision-making with legal or similar significant effects;
c. When conducting systematic monitoring;
d. When sensitive or highly personal data is involved;
e. When personal data processing relates to vulnerable data subjects;

---

[3] Section 28 (C & D) of NDPA.
[4] See, Anna Levitina, "Understanding Data Protection Impact Assessments Under The GDPR" available at <https://www.mondaq.com/data-protection/1416554/understanding-data-protection-impact-assessments-under-the-gdpr> accessed on 30th June 2025.
[5] See, <https://ndpc.gov.ng/wp-content/uploads/2025/03/NDP-ACT-GAID-2025-MARCH-20TH.pdf>accessed on 30th June 2025.
[6] Article 28 (3) of *NDPA-General Application and Implementation Directives* (GAID) 2025.

f. When considering the deployment of innovative processes or applications of new technological or organisational solutions which may pose a significant risk to the privacy of data subjects;
g. When developing software for the purposes of enabling communication with data subjects;
h. When engaging financial services involving the processing of personal data through digital devices;
i. When providing healthcare services;
j. When providing e-commerce services;
k. When deploying surveillance cameras in places that may be accessed by members of the public;
l. When developing and implementing any legal instrument or policy which requires the processing of personal data of members of the general public;
m. When engaging in educational services involving processing of various records relating to students or pupils;
n. When engaging in hospitality services; and
o. When engaging in cross-border data transfer.

Organizations undergoing or intending to conduct the above processing activities are obligated to conduct a DPIA to identify potential risks to the rights and freedoms of individuals and implement data protection solutions and measures to mitigate identified risks. The DPIA must be vetted by a certified Data Protection Officer (DPO), and the outcome of a DPIA should form a part of the NDP Act Compliance Audit Return (CAR) to be filed with the Commission.

The mode and implementation of a DPIA

Prior to the commencement of a project or a data processing activity, it is essential that an organization identify its objectives and the need for a DPIA. The organization should evaluate if the proposed project or data processing activity falls under the circumstances for conducting a DPIA. The mode of collection, processing, storage, and erasure of personal data must be clearly outlined to properly describe the data flow in the organization.

A standardized DPIA policy highlighting the process, procedures, criteria, and responsibilities for conducting DPIAs within the organization should be developed. The policy should conform to the provisions of the NDPA 2023, the GAID 2025, and international best practices.

A systematic assessment of privacy risks is conducted on the proposed project or data processing activities. This identifies the potential risks to the rights and freedoms of data subjects. Privacy Risk Assessment tools, procedures, and methodologies are utilized to evaluate and quantify the possible risks effectively.

Data protection solutions to prevent or mitigate the identified risks are proposed in a DPIA. Technical and organizational measures such as privacy-enhancing technologies and software, organizational processes, policies and procedures, contractual arrangements, and technical controls are developed to ensure effective and proportionate mitigation of the possible risks.

Essentially, the DPIA outcomes must be integrated into the proposed project or data processing activity. The remedial solutions and recommendations should be efficiently implemented into the project. Also, the processes and outcomes of the DPIA should be documented for accountability and transparency. The records of the DPIA must be kept for future occurrences and assessment.

The organization's DPO should collaborate with a licensed Data Protection Compliance Organization (DPCO) in conducting a DPIA for the company's data processing activities. Active involvement of relevant stakeholders in the company, such as IT professionals, Legal Officers, HR personnel, Compliance team, and Head of business units, is essential in identifying potential privacy risks and assessing the effectiveness of proposed mitigating measures recommended.

A significant mode of promoting the necessity of conducting a DPIA for certain companies in Nigeria, is the recent legal obligation imposed by the Federal Competition and Consumer Protection Commission (FCCPC) on Digital Lending Companies.[7] Digital Lending Companies are required to conduct a DPIA as a precondition to the approval of the company's registration.[8] Based on the data processing activities of digital lending companies, potential high-level risks are involved, and the likelihood of data breaches to the rights and freedoms of data subjects is inevitable. The mandatory DPIA imposed by the Commission ensures that possible risks are identified and evaluated based on the volume, variety, and sensitivity of the data, mode of processing, and protection mechanisms in place. The DPIA proposes effective remedial solutions to address the high-level risks detected prior to the commencement of operations by digital lending companies.

---

[7] The Commission issued a framework that regulates the digital lending space and makes provisions for the requirements for approval and registration to carry on the business of digital lending in Nigeria.

[8] See, FCCPC, *Limited Interim and Regulatory/Registration Framework and Guidelines for Digital Lending,* 2022 available at <https://fccpc.gov.ng/wp-content/uploads/2023/10/LIMITED-INTERIM-REGULATORY_-REGISTRATION-FRAMEWORK-FOR-DIGITAL-LENDING-2022.pdf> accessed on 3rd July 2025.

Conclusion

The DPIA is a vital tool in mitigating the potential impact of any security threats within an organization. A comprehensive and systematic DPIA conducted in an organization ensures effective management of privacy risks and compliance with data protection laws and regulations. DPIA addresses fairness and transparency in the organization's data processing activities and demonstrates the company's commitment to adhering to legal obligations and implementing data protection best practices. Organizations are encouraged to ensure early integration of DPIAs in their processing activities by conducting an assessment at the initial stages of the project planning to ensure that data protection measures are embedded in the proposed project. It is important to note that DPIAs are not one-off exercises; organizations are required to review and update their DPIA policy and conduct DPIAs periodically, especially with the introduction of new technologies and significant changes to the organization's data processing activities.

For further information on this article and area of law,
Please contact **Maryam Abdulsalam**
at: S. P. A. Ajibade & Co., Lagos by
Telephone (+234 1 472 9890), Fax (+234 1 4605092)
Mobile +234.908.819.3288, +234.903.967.5389
Email: mabdulsalam@spaajibade.com
www.spaajibade.com