THE DATA PROTECTION IMPACT ASSESSMENTS (DPIAs) UNDER GAID 2025: WHEN ARE THEY MANDATORY?

Aliu Oluwagbemisola Favour[1]

Faculty of Law, Adekunle Ajasin University

[1] **ALIU OLUWAGBEMISOLA FAVOUR, ADEKUNLE AJASIN UNIVERSITY**

ABSTRACT

In today's data-driven world, data breaches can affect hundreds of millions or even billions of people at a time. How can this be prevented or stopped? Well luckily there are laws put in place to regulate and help stop situations like these. The Global AI and Data Protection Regulation 2025 (GAID 2025) is an anticipatory law that safeguards and protects individuals' rights while mitigating institutional risk. GAID 2025 is a predecessor to, and replaced the the Nigeria Data Protection Regulation (NDPR) 2019. Data Protection Impact Assessment (DPIAs) play the role of spotting potential data breaches and security risks before it develops into a serious problem. They are preventive measures that identify, and mitigates or tackles head on privacy risk in data driven activities like; artificial intelligence, chat bots or Language Learning Models (LLMs) profiling users, powering fintance technology systems, managing sensitive health records, or running massive e-commerce engines,

This paper examines the exact situations where GAID 2025 makes DPIAs mandatory, while drawing comparisons with the General Data Protection Act (GDPR), Nigeria's Data Protection Act 2023, and the African Union's cybersecurity framework.

KEYWORDS

Data Protection Impact Assessments (DPIAs), GAID 2025, Artificial Intelligence (AI) Regulation, High-Risk Data Processing, Profiling and Automated Decision-Making.

INTRODUCTION

The emergence of advanced data technologies, particularly artificial intelligence has not only prompted the global community but also encouraged them to adopt more rigorous data protection standards, this is where GAID 2025 comes to play. GAID 2025 represents a comprehensive framework designed to regulate artificial intelligence (AI) and personal data processing on an international scale. One of its central compliance mechanisms is the Data Protection Impact Assessment (DPIA), which must be conducted whenever processing is likely to result in a high risk to individuals' rights and freedoms.[2] DPIAs serve as a required obligation, ensuring that risks are identified before high-risk operations begin. One of the most prominent features of the GAID 2025 is the expanded use of Data Protection Impact Assessments (DPIAS).

Comparatively, this approach aligns with the GDPR, which popularised DPIAs as a central accountability obligation.[3] The Nigerian Data Protection Act 2023 similarly emphasises risk-based regulation, reflecting a growing consensus on global best practice.[4]

2. DPIAs UNDER GAID 2025: LEGAL FRAMEWORK AND OBJECTIVES

According to GAID 2025, DPIAs is defined as structured assessments undertaken before initiating high-risk processing operations involving advanced automation, biometric data, or large-scale datasets and information. The objectives are fourfold: identifying risks, evaluating their impact, establishing safeguards, and demonstrating accountability to regulators.[5]

GAID 2025 is not only focused on widening the DPIA obligation beyond earlier legislation by introducing detailed AI-specific trigger systems. This expansion reflects concerns about unclarity, bias, and the potential for discrimination or data breaches inherent in automated systems.[6]

3. SCENARIOS IN WHICH DPIAs ARE MANDATORY UNDER GAID 2025

3.1 AI DEPLOYMENT AND AUTOMATED DECISION-MAKING

One prominent disadvantage of artificial intelligence (AI) systems, especially those used for predictive analytics and decision-making, is the potential of producing biased or prejudicial outcomes.[7] In situations like these, GAID 2025 mandates the use of DPIAs, for instance where; AI is used for decisions producing legal or similarly significant effects, such as employment screening, client profiling or loan approvals. Or in cases where Machine learning models rely on continuous personal data processing, this personal data could include, Sensitive information e.g., biometric or genetic information, which could end up being processed by AI systems.[8]

[2] Article 12, GAID 2025.
[3] Article 35, GDPR (EU 2016/679).
[4] GAID 2025, Part IV (DPIA Obligations).
[5] Edwards & Veale, *Enslaving the Algorithm* (CUP 2023).
[6] Wachter, Mittelstadt & Floridi (2017) 7 IDPL 76.
[7] GDPR, Recital 51.
[8] Bygrave, *Data Privacy Law* (OUP 2022).

Academic scholars have warned that algorithmic decision-making lacks transparency, increasing the need for formal assessments such as DPIAs.[9]

3.2 PROFILING AND BEHAVIOURAL TRACKING

Profiling is a psychological methodology that is used to get data about known or unidentified individuals or groups to assess their psychological characteristics. Profiling constitutes one of the most intrusive forms of data processing. DPIAs are mandatory under GAID 2025 where automated behavioural tracking, psychometric analysis, or real-time monitoring occurs.[10]

These risks are heightened in political advertising and consumer manipulation, where individuals may not fully understand the extent of monitoring.[11]

3.3 FINANCIAL SERVICES AND FINTECH OPERATIONS

The word “fintech” is simply a combination of the words “financial” and “technology”. It describes the use of technology to deliver financial services and products to consumers. These financial services depend heavily on data algorithms for risk scoring, fraud detection, and customer authentication. Have you ever wondered about how your banking app instantly recognizes you and shuts down if it senses an intruder? In cases like these, a lot of data protections are necessary for the protection of customers. GAID 2025 requires DPIAs in contexts involving: Algorithmic credit scoring, continuous monitoring of clients for fraud prevention, biometric banking authentication systems.

Because financial data is highly sensitive, regulators mandate encryption, pseudonymisation or anonymity, and algorithmic audit logs as mitigation tools.[12]

3.4 HEALTHCARE AND SENSITIVE DATA ENVIRONMENTS

In today's era, technology has now been implemented into the health sector, smart healthcare applies to any application or device that uses some combination of AI, sensors, data analytics, and networking to monitor patients' health conditions, inform clinical decisions, improve healthcare diagnostic research and services, connect care givers, and increase patient safety.

Healthcare data, genetic, biometric, diagnostic, is among the most sensitive categories of personal information. DPIAs are mandatory for prevention of AI-guided medical diagnostics, genetic profiling or biometric health monitoring, unethical sharing of patient data with insurers or pharmaceutical companies.[13]

The potential consequences of health data breaches justify a robust DPIA requirement.[14]. In this situation, GAID 2025 helps not only in the implementation but also reinforcement of right to privacy as provided by the1999 Constitution of The Federal Republic of Nigeria.

[9] GDPR, Article 22; NDPA 2023, s. 35.
[10] Tufekci, *Twitter and Tear Gas* (2017).
[11] NDPC Regulatory Guidelines (2024).
[12] African Union Data Protection Guidelines (2014).
[13] OECD AI Principles (2019).

3.5 E-COMMERCE SYSTEMS

E-commerce entails the buying and selling of goods and services over the internet. It involves all online activities related to these transactions, from initial product discovery to final purchase and payment, and includes a wide range of activities like online shopping, electronic payments, and online auctions.

This can be conducted through various platforms such as brand websites, mobile apps, online marketplaces like Amazon, and social media. E-commerce platforms conduct extensive tracking of consumer behaviour to aid goods' recommendations and improve their sales. Under GAID 2025, DPIAs are mandatory to curb situations like; the tracking of user behaviour across sites or devices, avoid recommendation engines that use personal data for profiling, and mitigate third parties such as advertisers or logistics companies from processing customer data.[14]

Data-driven retail creates risks of manipulation, discriminatory pricing, and unauthorised data exploitation.[15]

4. COMPARATIVE PERSPECTIVE: DPIAs IN OTHER REGULATORY REGIMES

4.1 GDPR (EUROPEAN UNION)

GDPR stands for General Data Protection Regulation, which is a comprehensive data privacy and security law enacted by the European Union (EU).

It provides a framework for how personal data can be collected, processed, stored, and transferred, and gives individuals more rights over their own data. The regulation was effected on May 25, 2018. GDPR prioritises individual consent before the processing of personal data.

Article 35 of the GDPR requires DPIAs where processing is likely to result in high risk, including large-scale profiling or monitoring.[16]

4.2 NIGERIA'S DATA PROTECTION ACT 2023

The Nigeria Data Protection Act 2023 is the country's comprehensive data protection law that establishes a groundwork for processing personal data and creates the Nigeria Data Protection Commission (NDPC) for enforceability.

This Act empowers the Nigeria Data Protection Commission to require DPIAs for high-risk AI, profiling, and biometric operations.[17] GAID 2025 introduces even stricter transparency duties, including mandatory algorithmic explanations.

4.3 AFRICAN UNION CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION

[14] EDPB DPIA Guidelines (2017).
[15] FPF "Impact Assessments in AI Governance" (2025).
[16] GDPR, Article 35(3).
[17] NDPA 2023, s. 31.

This landmark treaty aims to establish a comprehensive legal framework for cybersecurity, electronic transactions, and personal data protection across the African continent, this is indeed, a commendable feat.

However, while the AU Convention emphasises risk mitigation tools, it does not explicitly require DPIAs. GAID 2025 therefore fills a regional policy gap and provides harmonised standards across African jurisdictions.[18]

5. SIGNIFICANCE OF MANDATORY DPIAs

To foster continued effectiveness, I strongly opine that DPIAs should be made compulsory and sacrosanct for every institution or agency concerned. Although it does not eradicate all risks, a DPIA would help minimise and determine whether or not the level of risk is acceptable in the circumstances, and give the advantage of preparing a solution and planning ahead. DPIAs are a vital tool in reducing the potential impact of any security threats, these threats if not checked can affect billions of innocent consumers, lead to severe data leakage and different complications. Mandatory DPIAs strengthen; accountability, reasonable justification of high-risk decisions, early prediction of data mismanagement, transparency, ethical governance by ensuring fairness, non-discrimination, and data minimisation, regulatory compliance - since DPIAs can be audited or requested by authorities.[19]

In digital economies driven by automation, DPIAs act as a systemic check on misuse or unintended harm.

5.1 THE CHINESE SURVEILLANCE DATABASE CASE

The biggest ever data leak to date exposed 4 billion records, including WeChat data, bank details, and Alipay profile information of hundreds of millions of users, primarily from China, occurred in June 2025, The 631GB database - which also included phone

Numbers, home addresses, and behavioral profiles, was left wide open on the internet, unprotected by a password or any other form of authentication control. This was exposed by Bob Dyachenko, a cyber-security researcher who stumbled on billions of exposed records during a research project. The incident had an impact of over 4 billion records, researchers suggested that the leak was likely a centralised aggregation point for profiling, surveillance and data enrichment purposes.

6. CONCLUSION

Data Protection Impact Assessments under GAID 2025 serve as comprehensive ex ante safeguards in high-risk data processing environments. By mandating DPIAs for AI deployment, profiling, financial operations, healthcare systems, and e-commerce ecosystems, GAID 2025 reflects a global shift toward proactive, accountable data governance. As digital processes grow more complex, DPIAs remain indispensable for ensuring that innovation does not undermine fundamental human rights. One thing is certain, GAID 2025 is

[18] AU Convention (2014), Part III.
[19] OECD AI Principles / GAID 2025 Compliance Framework.

not just a regulation; it is a blueprint for trust and accountability in Nigeria's digital economy and across borders.

BIBLIOGRAPHY

1. Legislations

African Union Convention on Cybersecurity and Personal Data Protection (2014).

GAID 2025.

General Data Protection Regulation (EU) 2016/679.

Nigeria Data Protection Act 2023.

2. Books

Bygrave L, Data Privacy Law: An International Perspective (OUP 2022).

Edwards L and Veale M, Enslaving the Algorithm (CUP 2023).

Kuner C, Transborder Data Flows and Data Privacy Law (OUP 2021).

Tufekci Z, Twitter and Tear Gas (Yale UP 2017).

3. Cases

Chinese Surveillance Case

4. Journal Articles

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7 International Data Privacy Law 76.

5. Online Sources

(All accessed 22–23 November 2025)

European Data Protection Board, 'Guidelines on Data Protection Impact Assessment' https://edpb.europa.eu/our-work-tools.

Future of Privacy Forum, 'Impact Assessments in AI Governance' https://fpf.org/resources.

Nigeria Data Protection Commission, 'Regulatory Guidelines' https://ndpc.gov.ng/resources.

OECD, 'OECD AI Principles' https://oecd.ai/en/ai-principles.

European Union, 'GDPR Explained' https://europa.eu/dataprotection/gdpr.