

PRACTICE AREA / SECTOR GUIDELINE & OUTLOOK

(Nigeria)

1. Introduction to the Sector / Practice Area

The data protection and privacy landscape in Nigeria has evolved rapidly in recent years. With the enactment of the Nigeria Data Protection Act 2023 (NDPA) and the subsequent issuance of the General Application and Implementation Directive (GAID) 2025, organisations are now operating under a much stronger regulatory framework. In addition, Nigerians are becoming increasingly aware of their privacy rights and are willing to challenge how their personal data is handled.

Furthermore, the Nigerian Data Protection Commission (NDPC) has demonstrated a readiness to wield the “big stick” as seen in high-profile actions against entities such as MultiChoice and Meta, resulting in significant fines for various breaches of their data protection obligations. In light of this, data controllers and processors can no longer afford to treat data as a mere box-ticking exercise.

This Guide therefore provides readers with a bird’s-eye view of key issues and serves as a practical, hand-holding companion to Nigeria’s data privacy framework. The Guide addresses the key legislation and regulatory bodies responsible for data protection and privacy in Nigeria. It outlines the framework for reporting data breaches, rules for cross-border data transfers, and dispute-resolution principles governing data protection, the duties of data controllers and processors, the rights of data subjects, and specific restrictions imposed on data collection and processing activities. Further sections highlight the framework for reporting data breaches, rules for cross-border data transfers, and dispute resolution and enforcement mechanisms. The concluding chapters address emerging trends and offer an outlook on Nigeria’s data protection regime.

This Guide is designed to support data subjects in understanding their rights, assist data controllers and processors in understanding their responsibilities, anticipate regulatory expectations, and put the right structures in place to stay compliant and mitigate regulatory risk.

2. Key Definitions

The following includes key terminologies to note, as it relates to the data protection and privacy landscape:

a. Personal Data:

The Act defines Personal data as any information relating to an individual who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, social, cultural or economic identity of that individual.ⁱ

b. Data Subject:

This means an individual to whom personal data relates. It is further described as an “identified or identifiable natural person” from whom or about whom information is collected and/or processed.ⁱⁱ

c. Data Controller

This means an individual, private organisation, public Commission, agency or any other body/entity that, alone or jointly with others, determines the purposes and means of processing of personal data of data subjects.ⁱⁱⁱ

d. Data Processor

This means an individual, private entity/organisation, public authority, or any other body that processes personal data on behalf of, or at the direction of, a data controller or another data processor.^{iv} In simple terms, a data processor is the person who processes personal data on behalf of the data controller. They are usually external third parties authorised by the data controller to do so.^v

e. Data Controller or Processor of major importance

A data controller or processor of major importance, is described as a data controller or data processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate.^{vi}

Data controllers and processors of major importance are classified into three categories.

- i. **Ultra-high level:** An ultra-high level data controller and processor is an entity of major significance that is expected to adhere to the highest global standards of data protection, taking into account the highly sensitive personal data in their care, significant data-driven financial assets entrusted in them by the data subjects, reliance on third-party or cloud-based processing, engage substantially in cross-border data transfers, process personal data of more than 5,000 individuals, or require international certifications to ensure the confidentiality, integrity, and availability of data.^{vii}
- ii. **Extra-High level:** Extra-high level data controllers and processors are described as entities of significant importance that must comply with global best practices in data protection. Considering the handling of sensitive personal data in their care, managing data-driven financial assets entrusted in them by data subjects, performing government functions, relying on third-party or cloud-based processing, engaging in cross-border data transfers, processing personal data of more than 1,000 individuals,

or requiring recognised certifications to ensure the confidentiality, integrity, and availability of data.^{viii}

- iii. **Ordinary-High level:** An ordinary-high level data controller and processors are described as entities of notable importance that are required to adhere to global best practices in data protection, taking into account the sensitivity of data in their care, the inherent vulnerability of data subjects, or conducting systematic or automated processing that poses high privacy risks. It also includes those processing personal data of more than 200 individuals and those required to implement adequate technical and organisational measures, along with reputable certifications, to ensure data confidentiality, integrity, and availability.^{ix}

f. Consent

This means any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or to another individual on whose behalf he has the permission to provide such consent.^x It is the primary basis for the processing of personal data.

g. Data Breach

This means a breach of the security of a data controller or data processor leading to, or likely to lead to, the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.^{xi} In simple terms, a data breach, also known as a cyberattack, is any security incident in which unauthorised parties access sensitive or confidential information, including personal data of the data subjects.^{xii}

h. Processing of personal data

This means any operation or set of operations which is often performed on personal data, either by automated means, such as collection, recording, storage, adaptation, alteration, retrieval, use, disclosure by transmission, dissemination or not or by otherwise making available, alignment, combination, restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria.^{xiii}

i. Pseudonymisation

This means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.^{xiv} In simple terms, this is described as the process of replacing personal identifiers with aliases to protect privacy or security.^{xv}

j. Cross-border data transfer

This is described as the movement of personal data outside a country's jurisdiction, subject to specific data protection and privacy safeguards and regulations, such as the NDP Act 2023 or other safeguards of personal data in the jurisdiction to which the personal data is being transferred.^{xvi}

k. Privacy Policy

This is an organisation's way of communicating with its online users and potential visitors in clear, concise, and unambiguous language, aimed at providing users with a better understanding of its data processing and collection practices.^{xvii}

l. Purpose Limitation

This principle of data processing requires that personal data be collected for a specified, explicit, and legitimate purpose, and not further processed in a way incompatible with these purposes.^{xviii}

m. Data Minimisation

This is a fundamental principle of data processing, which requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is collected or further processed.^{xix}

n. Storage Limitation

This is a fundamental principle of data processing, which requires that data be retained for no longer than is necessary to achieve the lawful basis for which the personal data was collected or further processed.^{xx}

o. Integrity and Confidentiality

This is a fundamental principle of data processing, which requires that personal data be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.^{xxi}

p. Lawfulness, transparency, and fairness

This means that personal data, as a critical digital asset, is expected to be processed in a lawful, transparent, and fair manner.^{xxii}

q. Data Protection Impact Assessment

This is described as a process designed to identify the risks and impact of the envisaged processing of personal data.^{xxiii}

r. Cookies

Cookies are small text files used on websites to store a wealth of data, potentially identifying website visitors without continuous consent. Essentially, they serve as a primary tool for advertisers to track the online activity of data subjects visiting their website.^{xxiv}

s. Data Protection Officer

A data protection officer ensures that the organisation processes the personal data of its staff, customers, providers, or other data subjects in compliance with data protection laws and regulations.^{xxv}

t. Data Privacy Impact Assessment

This is an assessment that is expected to be undertaken by a data controller or processor where the processing of personal data may likely result in a high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purpose.^{xxvi}

u. Data Protection Compliance Organisation

This is defined as any entity duly licensed by the Nigerian Data Protection Commission (NDPC) for the purpose of training, auditing, advising, and rendering services aimed at ensuring compliance with the NDP Act 2023 or any foreign Data Protection law or regulation having effect in Nigeria.^{xxvii}

ACRONYMS

Acronym	Meaning
G.D.P.R	EU General Data Protection Regulation
NDPC	Nigerian Data Protection Commission
NDP Act	Nigeria Data Protection Act 2023
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
PII	Personally Identifiable Information
DPCO	Data Protection Compliance Organisation
AI	Artificial Intelligence
IoT	Internet of Things
ISO	International Organization for Standardization
GAID	NDP Act 2023 General Application and Implementation Directive
SCC	Standard Contractual Clauses
UHL	Ultra-High Level
EHL	Extra-High Level
OHL	Ordinary-High Level

3. Key Legislation

The legislation governing data protection in Nigeria comprises primary legislation, subsidiary regulations, and sector-specific rules that govern how personal data is collected, used, shared, and protected. The primary legislation governing is the Nigeria Data Protection Act 2023 (NDPA), supported by guidelines, directives, and specialised rules issued by the Nigerian Data Protection Commission (NDPC) and other regulators whose mandates intersect with privacy and data governance.^{xxviii}

a. Nigeria Data Protection Act 2023 (NDPA)

The NDPA is the central legal instrument governing data protection in Nigeria. The Act is Nigeria's first data protection law, built on the earlier Nigeria Data Protection Regulation of 2019 and its 2020 implementation framework.^{xxxix} It establishes rights for data subjects, sets out lawful bases for processing, prescribes data protection principles and outlines the duties of data controllers and processors for the protection of personal information.^{xxx} The Act also establishes a ranking system to classify controllers and processors based on the significance of the data they process, enhances requirements for reporting data breaches, sets rules for cross-border data transfers, and requires the appointment of Data Protection Officers in certain circumstances.^{xxxi} The Act establishes the Nigerian Data Protection Commission as the official body tasked with overseeing the sector, enforcing compliance, and shaping relevant policies. It also equips the Commission with investigative powers, allowing it to issue compliance directives and impose administrative penalties where necessary.^{xxxii}

- b. General Application and Implementation Directive (GAID):** This directive became effective on September 19, 2025, and replaced the previous Nigeria Data Protection Regulation (NDPR) 2019.^{xxxiii} It offers clear and practical guidance on the responsibilities of data controllers and processors, including the proper documentation of processes, expectations for Data Protection Impact Assessments (DPIAs), and the establishment of effective data governance frameworks.^{xxxiv}

4. Regulatory Authorities and Sector-specific Legislations

Various regulatory authorities exercise powers that involve personal data within their areas of responsibility. The sector-specific regulations operate in conjunction with the NDPA and NDPC directives. Such sector-specific legislations and authorities are:

a. The Nigeria Data Protection Commission (NDPC)

The NDPC, established under Section 4 of the NDPA, is the primary regulatory authority for data protection in Nigeria. It succeeded the Nigeria Data Protection Bureau (NDPB) and now functions as an independent statutory body with perpetual succession and corporate personality. The Commission's functions, set out in Section 5, include: Overseeing implementation of the NDPA and subsidiary instruments; Accrediting Data Compliance Service Providers (DCSPs) and Data Protection Compliance Organisations (DPCOs); Registering DCPMIs; Investigating violations and imposing administrative penalties; Advising government on data protection policy and Promoting public awareness and stakeholder engagement. The NDPC's enforcement powers derive from Sections 46–53, which empower it to issue enforcement orders, impose administrative fines, and conduct audits or investigations either suo motu or upon complaint.

b. Central Bank of Nigeria (CBN)

Financial institutions are required to comply with CBN regulations on cybersecurity, outsourcing, payment systems and KYC procedures, all of which involve strict handling of customer data. The CBN Cybersecurity Framework and the Risk-Based Cybersecurity Framework for Deposit Money Banks set standards for data security and incident reporting.^{xxxv}

c. National Information Technology Development Agency (NITDA)

While the NDPC now takes the lead on data protection, NITDA still plays a key role in shaping broader ICT policies. This includes guidance on cloud computing, cybersecurity, and frameworks for digital platforms. These policies often overlap with privacy requirements, particularly for organisations that rely heavily on technology.

d. Nigerian Communications Commission (NCC)

Telecommunications operators must adhere to NCC's Consumer Code of Practice Regulations, the Data Protection Regulations for Communications Licensees and SIM registration rules. These guidelines impose obligations relating to subscriber information, retention periods, access logs and disclosure procedures.^{xxxvi}

e. National Health Insurance Authority (NHIA) and Federal Ministry of Health

Health authorities oversee health-related data through frameworks like the National Health Act, e-health standards, and guidelines for digital health records. These rules focus on protecting patient confidentiality, securing consent, managing data retention, and ensuring sensitive health information is handled responsibly.^{xxxvii}

f. Securities and Exchange Commission (SEC) & Investment and Securities Act

Entities in the capital markets ecosystem must comply with SEC cybersecurity guidelines and investor-protection rules governing the handling of financial, biometric, and transaction data. For instance, the Investment and Securities Act 2025 strengthens governance and requires disclosure of beneficial ownership and ensures compliance with AML/CFT obligations for trustees and corporate service providers. Going forward, the regulatory and legislative framework for trusts and fiduciary services in Nigeria will remain closely guided by the ISA 2025.^{xxxviii}

5. Principles of Data Protection

Data Protection principles are the core values that guide the collection, processing, and storage of personal data of a data subject. They serve as the compass for data controllers and data processors when handling personal data, thus providing the blue print for compliance.^{xxxix} These principles are outlined in various data protection legislations, for example, the *General Data Protection Regulation 2018 (GDPR)* and the *Nigeria Data Protection Act 2023*, establish these principles as follows:

a. Lawfulness, Fairness & Transparency:

Lawfulness, in this context means that personal data must only be processed where there is a valid legal basis for doing so. The Nigeria Data Protection Act 2023 outlines six lawful bases under which personal data may be processed, which include: Consent,^{xi} performance of a contract^{xli}, compliance with a legal obligation^{xlii}, protection of vital interests,^{xliii} public interest or official authority^{xliiv} and legitimate interest.^{xliv}

Additionally, the processing of personal data will be deemed unlawful where: It overrides the fundamental rights, freedoms, and interests of the data subject, thereby infringing on their dignity or privacy;^{xlvi} it is incompatible with the lawful bases of processing stipulated under the law^{xlvii} and where the data subject could not reasonably expect or envisage that their personal data would be processed in the specific manner, being undertaken, especially where such processing lacks transparency or veers from the original stated purpose^{xlviii}

Fairness requires that personal data be processed in a way that is fair and with respect to the rights and dignity of the data subject.^{xlix} Their data should not be processed in a manner that is misleading, manipulative, or that could cause harm to the data subject. Additionally, the data subject must have a reasonable expectation of how their data will be used.ⁱ

Transparency, in the context of this principle, requires that any information provided to data subjects be concise, easily accessible, and easy to understand.ⁱⁱ It further requires the use of clear and plain language, and, where appropriate, visualisation.ⁱⁱⁱ For example, a data controller on their website should present its privacy notice in plain language, using short sentences or icons to explain why the data is needed and how it will be used, rather than hiding that information in lengthy, complex legal text.

b. Purpose Limitation

This principle implies that personal data must be collected for a specified, explicit, and legitimate purpose, and should not be processed in a way incompatible with these purposes.ⁱⁱⁱⁱ This principle ensures that organisations remain transparent about why they collect personal data, which in turn helps build trust with data subjects. It also reinforces individuals' right to control how their information is used, as they can give informed consent for a clearly defined purpose.

c. Data Minimisation

This requires that personal data be adequate, relevant, and limited to what is necessary for the purposes for which it is collected or further processed.^{liv} The core elements of this principle include: purpose limitation,^{lv} Data Accuracy,^{lvi} Limiting Use,^{lvii} and Retention Limitation.^{lviii}

d. Storage Limitation

The law requires that data be kept only as long as necessary to achieve the lawful basis for which the personal data was collected or further processed.^{lix} Therefore, once the data is no longer required for that specific purpose, it should be deleted or anonymised.^{lx}

e. Accountability^{lxi}

The principle of accountability mandates that a data controller or data processor owes a duty of care in respect of data processing and shall demonstrate accountability in respect of the principles contained in this Act.^{lxii} To comply with this principle, data controllers and processors are encouraged to implement the following:

- i. Maintain a Record of Processing Activities (ROPA) detailing all personal data processing activities;^{lxiii}
- ii. Create and regularly update data protection policies to ensure continued effectiveness;^{lxiv}
- iii. Have written contracts with data processors and third parties;^{lxv}
- iv. Implement appropriate technical and organisational security measures;^{lxvi}
- v. Provide clear privacy notices to data subjects;^{lxvii}
- vi. Conduct Data Protection Impact Assessments (DPIAs) for high-risk processing to identify and reduce potential data protection risks.^{lxviii}

f. Integrity and Confidentiality

The principle of integrity and confidentiality requires personal data to be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.^{lxix} Similarly, a data controller and data processor should implement appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data.^{lxx} Some of these measures include pseudonymisation and encryption of personal data.

g. Accuracy

This generally requires personal data to be accurate, complete, not misleading, and, where necessary, kept up to date, taking into account the purposes for which the data is collected or further processed.

6. Obligations of Data Controllers and Processors

The NDPA 2023 imposes certain responsibilities on data controllers and processors to ensure that personal data is handled lawfully, fairly, and transparently. GAID 2025 further interprets and clarifies these obligations, providing operational guidance on compliance. These obligations include:

a. Duty to Establish a Lawful Basis for Processing

Before processing any personal data, controllers and processors must identify and document the specific lawful basis justifying the processing. The NDPA recognises six lawful bases, namely: Consent, Performance of a contract or pre-contractual steps, Compliance with a legal obligation, Protection of vital interests, Performance of a public task or exercise of official authority, Legitimate interests of the controller, processor, or a third party. These factors guide the scope and limits of data processing and must be communicated in clear privacy notices.

b. Data Retention and Deletion Obligations

Under the Nigeria Data Protection Act 2023, data controllers and processors must not retain personal data longer than necessary.^{lxxi} While the Act does not define what constitutes a “necessary” retention period, earlier guidance under the NDPR Implementation Framework provided indicative timelines, such as three years after last platform use or six years after the last contractual transaction but these timelines no longer apply following the introduction of the GAID.^{lxxii} Although the GAID does not prescribe specific retention periods, it emphasises purpose limitation and defines “retain” as holding personal data only for specified, explicit, and legitimate purposes.^{lxxiii} Once those purposes have been fulfilled or abandoned, the legal basis for continued retention ends.

c. Data Breach Reporting & Response Framework Obligations

Data controllers and processors have a duty to ensure the security, confidentiality, and integrity of personal data.^{lxxiv} They must adopt appropriate technical and organisational measures to prevent accidental or unlawful destruction, loss, misuse, alteration, or unauthorised access by maintaining a strong data breach prevention and response framework.^{lxxv} Nigeria’s data breach reporting obligations are primarily set out in the NDPA 2023 and the Cybercrimes Act 2015 (as amended in 2024). In the NDPA, Data controllers and processors must report personal data breaches to the NDPC within 72 hours of becoming aware of the breach. If the breach poses a likely risk to individuals’ rights and freedoms, affected data subjects must also be notified without delay. Non-compliance may attract significant penalties.^{lxxvi} In the Cybercrimes Act, any individual or institution that experiences a cyberattack, intrusion, or system disruption must notify the ngCERT Coordination Centre (through sectoral CERTs or SOCs) within 72 hours of detection.^{lxxvii}

d. Cross-Border Transfer of Data

Given the global nature of business, transferring personal data across borders is often essential. The NDPA requires data controllers and processors to ensure that such transfers provide adequate protection for the data subject. Under the NDPA, personal data cannot ordinarily be transferred outside Nigeria except where the controller or processor confirms that:^{lxxviii}

- i. The recipient is governed by a law or framework that provides adequate protection for personal data. This may include legislation, binding corporate rules, contractual clauses, codes of conduct, or certification mechanisms that meet the NDPA's standard of adequacy ("Adequacy Decision").
- ii. A recognised transfer instrument exists between the NDPC and the foreign authority that guarantees sufficient safeguards.
- iii. Another lawful basis for the transfer applies under the Act.^{lxxxix}

Controllers and processors must also document the legal basis relied upon for any cross-border data transfer.

e. Accountability and Governance

The NDPA adopts an accountability-based model that requires organisations to demonstrate compliance, not merely assert it. Accordingly, data controllers must maintain proper records and implement governance structures that show active adherence to statutory obligations. This includes appointing a Data Protection Officer (DPO), where required, to oversee internal compliance programmes;^{lxxx} conducting Data Protection Impact Assessments (DPIAs) for high-risk or sensitive processing activities to identify, prevent, or mitigate privacy risks;^{lxxxi} and filing annual Compliance Audit Returns (CARs) with the NDPC.^{lxxxii}

Data processors, on their part, must act strictly on the documented instructions of controllers and implement appropriate technical and organisational measures that mirror the controller's obligations. They are also expected to maintain processing records, support DPIA processes, and ensure that subcontractors or third parties meet equivalent data-protection standards.^{lxxxiii} Together, these measures underscore the NDPA's shift toward continuous, accountable, and evidence-based compliance.

7. Rights of Data Subjects

Data subject rights are enshrined under *Parts VI and X* of the *NDPA, 2023*, and further elaborated in the *GAID, 2025*. While the former establishes the foundational principles and legal entitlements of data subjects, the latter provides detailed practical guidance for the enforcement of these rights. Taken together, the *NDPA* and *GAID* form a comprehensive and 'rights-driven' framework that substantially reflects international data protection regimes and best practices, particularly the *EU GDPR*.

The rights include:

a. The Right to be informed

Sections 27 and 34(1)(a) of the Nigerian Data Protection Act, 2023, give data subjects the right to be informed about the collection and processing of their personal data. The right is primarily derived from *Section 24(1)(a) of the NDPA*, which mandates that personal data

be processed “in a fair, lawful, and transparent manner.”^{lxxxiv} The essence of the transparency principle and the right to be informed is to ensure data subjects are aware that their personal data is being collected and processed. It also ensures that they are aware of the purpose of the collection and the other rights available to them in relation to the processing of their data.^{lxxxv}

b. The Right to Access Personal Data

The right of access set out in *Section 34(1)(b) of the NDPA, 2025*, grants data subjects the authority to request and be informed of their personal data in the custody of data controllers, including information on how the data is stored and processed. This is why this right is considered as the “active counterpart to the more passive right of information.”^{lxxxvi} Accordingly, a data subject has the right to request and obtain, in a concise, intelligible, and commonly used electronic format,^{lxxxvii} information about the extent and use of its personal data from the data controller.^{lxxxviii}

c. The Right to Rectification of Personal Data

The right to rectification emphasises the principle of data accuracy under the *NDPA*.^{lxxxix} It provides data subjects with the right to seek the correction of inaccurate personal data held by the data controller. This right to rectification is expressly provided in *Section 34(1)(c) of the NDPA, 2023*.

d. The Right to Object to the Processing of Personal Data

The right to object to the processing of personal data is an essential tool for the enjoyment of the right to privacy. Under *Section 36 of the NDPA*, a data subject has the right “to object to the processing of personal data relating to the data subject.” The Act considers processing activities to include direct marketing or profiling for direct marketing.^{xc}

Where this right is exercised, the data controller must discontinue the processing of personal data, as failing to do so could result in liability for violating the right to privacy.

e. The Right to Withdraw Consent

Section 35 of the NDPA provides for the right of a data subject to withdraw their prior. Once consent is withdrawn, the data controller must cease any processing of that personal data. The NDPA also emphasises that the procedure for exercising the withdrawal should be as simple and straightforward as it was to give the consent.

f. The Right to Restrict the Processing of Personal Data

The right to the restriction of processing of personal data means that the organisation (data controller or processor) must temporarily limit or pause the use of a person’s personal data until certain issues are resolved, including:

- i. The resolution of any request made by the data subject in relation to that particular personal data or processing activity;
- ii. Objection to processing activities made by the data subject under the *NDPA*. In this instance, the right to restriction is complementary to the right to objection, and need not be expressly sought; or
- iii. The establishment, exercise, or defence of legal claims relating to the data subject.^{xcii}

g. The Right to Portability

The right to portability essentially enhances the rights to information and access. Portability enables data subjects to obtain and transfer their personal data easily. This right can be exercised in three different ways:

- i. The right to request and receive, without undue delay from a data controller, personal data concerning the data subject in a structured, commonly used, and machine-readable format. ^{xciii}
- ii. The right to transmit the personal data which the data subject received to another data controller without any hindrance. This should also be done without any interference or unreasonable delays from the data controller.
- iii. The right to request that a data controller transmit the personal data directly to another, where it is technically feasible to do so.^{xciii}

h. The Right to Lodge a Complaint

This is an enforcement mechanism established under *Section 46 of the NDPA*. It enables a data subject to seek administrative redress for data rights breaches or processing that contravenes the provisions of the *NDPA*. A data subject can lodge a formal complaint with the NDPC where it believes or suspects that its rights have been or are at risk of being breached by a data controller or processor.^{xciv} Upon receiving the complaint, the Commission has a duty to investigate and address it within the bounds of the law.^{xcv}

i. The Right not to be Subjected to Automated Decision-Making

Before the introduction of the *NDPA*, the obligation regarding automated decision-making was limited to notifying the data subject of its use. Now, under *Section 37 of the NDPA*, a data subject has the right not to be subjected to a decision based solely on automated processing of personal data, including profiling, which has legal implications for the data subject. It is important to highlight that this right is quite limited and applies only when the decision *will have legal consequences for the data subject*.

8. Restrictions to Data Collection and Processing

The *NDPA* introduces deliberate and robust limitations on how personal data may be collected and processed, ensuring that organisations operate within clearly defined ethical and legal boundaries. These restrictions reflect core data protection principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation,

accountability, and confidentiality and are critical to safeguarding the rights and freedoms of data subjects.

Some examples include:

a. CCTV and Video Surveillance

CCTV deployment is subject to strict legal controls to prevent excessive or intrusive monitoring. Organisations must carry out a Data Protection Impact Assessment (DPIA) before installation^{xcvi}, use conspicuous signage to inform individuals of the surveillance, and ensure that camera placement does not violate reasonable expectations of privacy (e.g., bathrooms, changing rooms, private offices) in line with global best practices. Retention of footage must be time-bound and secure, and access should be restricted to authorised personnel.

b. Child Data Protection

Children enjoy heightened privacy protection due to their vulnerability. Under the NDPA^{xcvii}, Data Controllers must obtain verifiable parental or guardian consent before processing a child's personal data, unless a narrowly defined exception applies^{xcviii}. Data collection from children must be limited to what is strictly necessary, and entities are prohibited from engaging in behavioural profiling, targeted advertising, or automated decision-making that produces significant effects on a child. It is important to note that in Nigeria, Data processing for Children must be done in a manner consistent with the Child's Right Act 2003^{xcix}.

c. Employee Monitoring

Employee monitoring must respect the constitutional right to privacy under Section 37 of the Constitution of the Federal Republic of Nigeria. Employers may use tools like email monitoring, CCTV, biometrics, GPS, or productivity software only when necessary and for legitimate purposes such as security or fraud prevention. They must clearly inform employees about what is being monitored, why, and the legal basis for doing so^c, while using the least intrusive methods. Any monitoring that violates employees' dignity or autonomy, or involves unjustified or continuous surveillance, is considered unlawful and incompatible with proper workplace practices. It is important to note that organizations that are involved in Employee Monitoring are mandated to undertake a Data Privacy Impact Assessment (DPIA) as it may likely result in high risk to the rights and freedoms of the Employees by virtue of its nature, scope, context, and purposes^{ci}.

d. Sensitive Personal Data Restriction

The NDP Act^{cii} defines sensitive personal data as data relating to an individual's genetic and biometric data, race or ethnic origin, religious beliefs, health status, sex life, political opinions or affiliation, trade union membership. The NDP Act restricts processing of sensitive personal data unless explicit consent has been gotten from the data subject^{ciii} or a statutory exception exists^{civ}. Such data must be subject to enhanced safeguards,

including encryption, access logging, and stricter retention controls^{cv}. Organisations must demonstrate compelling necessity before handling this category of data.

e. Cross-Border Transfer Restrictions

Personal data may not be transferred outside Nigeria except to jurisdictions with adequate data protection safeguards or where specific mechanisms such as contractual clauses, codes of conduct, binding corporate rules^{cv}, or explicit consent are in place^{cvii}. Even then, the data exporter must ensure ongoing protection equivalent to the NDPA standard^{cviii}.

f. Limitations on Data Retention

Data retention must be strictly time-bound and data must not be retained for longer than is necessary^{cix}. Organisations may not keep personal data longer than necessary for the original purpose of collection. Organisations must have clear data retention/data storage policies^{cx}. The data retention policies must be documented, justified, and periodically reviewed and communicated clearly to data subjects^{cx}. It is important to note that the information to data subjects in respect of data retention must clearly indicate the implication for Data Subject's Access Request (DSAR)^{cxii}.

g. Restrictions on Sharing with Third Parties

Personal data may not be shared with third parties including contractors, affiliates, regulators, or law enforcement unless a lawful basis for such disclosure exists. Where third-party sharing is permitted, the data subject's explicit consent must be obtained, and the purpose, scope, and duration of the sharing must be clearly communicated. Individuals must also retain the right to withdraw their consent at any time^{cxiii}.

9. Reporting Data Breaches

The obligation to report personal data breaches is one of the most critical accountability mechanisms under the Nigeria Data Protection Act, 2023 ("NDPA"). Section 40 of the Act establishes a structured, time-sensitive incident-response framework that mandates early notification, coordinated containment, and transparent communication with regulators and affected individuals. Article 33 of the General Application and Implementation Directive, 2025 ("GAID 2025") further expands this framework by clarifying the risk thresholds, notification content, and expectations for regulatory cooperation. Together, these instruments reflect Nigeria's alignment with global best practices in data breach governance.

Under the Act, the first responsibility lies with the data processor. Once a processor becomes aware of a breach affecting personal data under its care, it must immediately notify the data controller or the processor that engaged it.^{cxiv} This notification must describe "the nature of the personal data breach including, where possible, the categories and approximate numbers of data subjects and personal data records concerned"^{cxv}. It must also respond to all information requests necessary for compliance.^{cxvi}

The core notification duty rests on the data controller. Under Section 40(2), a controller must notify the Nigeria Data Protection Commission (NDPC) “within 72 hours of becoming aware of a breach which is likely to result in a risk to the rights and freedoms of individuals.” The controller must also, where feasible, describe the nature of the breach and estimate the categories and numbers of affected data subjects and records. GAID 2025 reinforces this timeline, with Article 33(1) explicitly reiterating the 72-hour notification requirement.

Where the breach is likely to pose a high risk to data subjects, the Act obliges the controller to “immediately communicate the personal data breach to the data subject in plain and clear language.”^{cxvii} The communication must provide advice on measures the individual may take to mitigate harm. Where direct contact is not feasible or would involve disproportionate effort, Section 40(3) allows for a public announcement through widely used media sources. GAID 2025 clarifies what constitutes high risk: under Article 33(2), a breach is considered high risk when the nature of the breach makes victims susceptible to fraud, identity theft, or exposure of sensitive personal data.

Both the Act and the Directive specify what notifications must contain. Under the Act, communications to controllers, the Commission, or data subjects must include:

- i. the name and contact details of a point of contact;
- ii. a description of the likely consequences of the breach; and
- iii. the measures taken or proposed to address the breach and mitigate its effects.^{cxviii}

GAID 2025 expands on this list in Article 33(5), requiring descriptions of how the breach occurred, the time period involved, the nature of the personal information compromised, a formal risk assessment, the number of individuals facing significant harm, and the steps taken both to reduce harm and to notify affected persons.

GAID 2025 also introduces an enhanced duty of care. Under Article 33(4), controllers and processors are required to provide immediate notification to relevant authorities, including the NDPC, if early disclosure could help contain imminent or large-scale national risks, irrespective of the statutory 72-hour window in Section 40(2). This reflects the Directive’s practical and preventive orientation.

Documentation is an essential compliance obligation within the NDPA. Controllers and processors must “keep a record of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.”^{cxix} These records must be sufficient for the Commission to verify compliance. Additionally, Section 40(5) empowers the NDPC to issue public communications where a controller’s efforts to notify data subjects are inadequate, while Section 40(6) mandates the Commission to issue further regulations on appropriate methods of notification.

Collectively, Section 40 of the NDPA and Article 33 of GAID 2025 establish a comprehensive and risk-based approach to reporting data breaches in Nigeria. They emphasise prompt notification, clear communication, thorough documentation, and the protection of individuals' rights. In an era of growing cyber vulnerabilities, this framework ensures that organisations adopt proactive and accountable practices, strengthening trust in Nigeria's data governance environment.

10. Enforcement, Sanctions and Dispute Resolution

The Nigeria Data Protection Act ("NDPA") provides for dispute resolution and enforcement mechanisms in cases of breach of any of the rights and/or obligations provided under the NDPA. The options available to a data subject whose right has been infringed upon by a data controller or data processor are as discussed below.

Available Dispute Resolution Mechanisms Under The Nigeria Data Protection Act

a. Complaints to the Nigeria Data Protection Commission

A data subject whose right has been violated or likely to be violated reserves the right to lodge a complaint with the Commission.^{cxix} Where Commission finds merit in the complaint, the Commission may investigate the complaint. Notably, the Commission may also initiate an investigation on its own accord where it believes that a data processor or controller has violated, or is likely to violate, the provisions of the NDPA.^{cxxi}

Upon receipt of the complaint, the Commission may order the person against whom the complaint was made to appear for the purpose of being examined orally, produce documents as may be required, and/or furnish a statement in writing made under oath or an affirmation setting out all the required information.

Furthermore, where a violation of the provisions of the NDPA has been established and the Commission is satisfied that a data controller or data processor has violated or is likely to violate any requirement under the Act, the Commission may proceed to make an appropriate compliance order in writing against the data processor or data controller.^{cxxii}

The compliance order may be in form of warning, a requirement that the data controller or data processor should comply with the relevant provisions of the NDPA or cease and desist order requiring the data controller or data processor to refrain from doing an Act.^{cxxiii}

Apart from the compliance order which the Commission may make, by the provisions of Section 48 of the NDPA, if the Commission, after completing an investigation under section 46 of the NDPA, is satisfied that a data controller or data processor has violated any provision of the NDPA or subsidiary legislation made under the NDPA, the

Commission may make any appropriate enforcement order or impose a sanction on the data controller or data processor; and shall inform the data controller or data processor, and if applicable, any data subject who lodged a complaint leading to the investigation, in writing of its decision.^{cxxiv}

Notably, in respect of the penalty or remedial fee payable in cases of violation, the “higher maximum amount” which shall be greater of NGN10, 000, 000, and 2% of the annual gross revenue in the preceding year shall be payable, in the case of a data controller or data processor of major importance or the standard maximum amount, which shall be greater of NGN2,000,000 and 2% of the annual gross revenue in the preceding year in the case of a data controller or data processor not of major importance.^{cxxv}

- b. Judicial Review:** A person who is not satisfied with an order of the Commission may apply to the court for judicial review within 30 days after the order was made.^{cxxvi}
- c. Civil Remedies:** By the provision of Section 51 of the NDPA, a data subject, who suffers injury, loss, or harm as a result of a violation of the NDPA by a data controller or data processor, may recover damages from such data controller or data processor in civil proceedings.
- d. An order for forfeiture:** Where a data processor or controller is convicted, the Court may make an order of forfeiture against the convicted data controller, data processor, or individual in accordance with the Proceeds of Crime (Recovery and Management) Act.^{cxxvii}

11. Trends and Outlook

Data protection trends are increasingly shaped by stronger enforcement and higher compliance expectations, as regulators focus on supervision, accountability, and meaningful sanctions rather than new legislation. Organisations are now expected to demonstrate practical and well-documented privacy governance.

In addition, Artificial intelligence has become a key driver of change, with data protection increasingly integrated into AI governance through requirements for transparency, risk assessment, and human oversight. At the same time, data sovereignty is gaining prominence, as stricter cross-border transfer rules and local-storage expectations reshape how data is managed, particularly in sensitive sectors.

Overall, data protection is no longer viewed solely as a legal obligation but as a core governance and risk issue, closely linked to trust, corporate responsibility, and organisational resilience.

In terms of the Outlook, Nigeria's data protection regime has moved from formation to operational maturity, with the focus shifting from new laws to rigorous, coordinated, and strategic enforcement. The coming months will be shaped by stricter implementation of the GAID, deeper regulatory harmonisation, risk-based enforcement, and growing judicial engagement, all of which will raise compliance expectations across sectors. Regulatory attention will center on full GAID enforcement, including standard contractual clauses, sector-specific codes of conduct, enhanced audit requirements, and the professionalisation of DPOs and DPCOs. The NDPC is also expected to intensify coordination with regulators such as the CBN, NCC, FCCPC, and SEC, reducing fragmentation while expanding enforcement reach, particularly in fintech, telecoms, and digital platforms.

Open Banking will test consent structures, data-sharing controls, and liability allocation, with joint NDPC-CBN enforcement likely. Sanctions will become more predictable through a consolidated enforcement framework, even as high-profile actions against major platforms continue.

Legislatively, activity will increase but may create regulatory density, with NDPA amendment bills, digital-economy legislation, AI governance proposals, cybersecurity reforms, and child online protection laws advancing in parallel.

Market impacts will include growth in privacy and compliance services, increased pressure for local data hosting, closer alignment between data protection, ESG, and corporate governance, and a shift toward consent-driven digital business models. AI governance will mature through overlapping NDPC and NITDA oversight, risk-based AI classification, and sector-specific guidance.

Litigation is expected to rise as courts engage more substantively with data protection claims, increasing damages exposure. Finally, 2026 is likely to see clearer international data-transfer mechanisms, supporting cross-border data flows and Nigeria's deeper integration into the global digital economy.

Firm's Profile

Kenna is licensed by the Nigerian Data Protection Commission as a Data Protection Compliance Organisation to provide monitoring, auditing, training, and data protection compliance services to organisations. Our Firm has advised a wide range of companies on data protection and data privacy. We advised companies on the Nigeria Data Protection Act (NDPA) 2023 and the General Application and Implementation Directive (GAID) with a specific focus on consumer consent, data controllers, and data processing. Very recently, the firm has published an authoritative book on Data Protection, titled *Legal And Regulatory Aspects of Data Protection*.

Kenna also publishes and writes articles on data protection in Nigeria as part of our contribution to deepening the knowledge pool in this area. As issues of digital protection become increasingly pertinent, the firm ensures it stays abreast of digital marketplace trends and emerging regulations/laws. We also regularly advise on the General Data Protection Regulation (GDPR), which applies to individuals who live in the European Union (EU) region and even beyond, and critically analyse its applicability to our clients, both international and domestic.

Our firm has represented several clients in data protection and privacy. One such company is a medical technology company in partnership with a foreign company, for which we advised on the use of customer data. Our team advised a telemedicine/ digital health company on the provisions of the Nigerian Law on Data privacy and Data protection, including the NDPA 2023 and other extant data privacy and protection regulations. We provided the company with legal advice on the necessary steps to ensure that the personal data collected from potential patients/users is properly managed in accordance with Nigerian law and international best practices on data management.

Kenna remains committed to supporting organisations in navigating the complexities of data protection landscape. We assist organisations in understanding and remaining compliant with their obligations under the extant laws.

Contact details of key partners or practice leads



Nimma Jo- Madugu

Partner

njo-madugu@kennalp.com



Chidera Ezenwanne

Senior Associate

cezenwanne@kennalp.com



Oluwapelumi Ikujenyo

Associate

oikujenyo@kennalp.com

Endnotes

- ⁱNigeria Data Protection Act 2023, Section 65.
- ⁱⁱEU General Data Protection Regulation 2018, Article 4.
- ⁱⁱⁱNigeria Data Protection Act, Section 65.
- ^{iv}Nigerian Data Protection Act, Section 65.
- ^vEuropean Commission, “What is a data controller or a data processor?” https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en > accessed October 16, 2025.
- ^{vi}Nigeria Data Protection Act 2023, Section 65
- ^{vii} Nigeria Data Protection Commission, “Guidance Notice: Registration Of Data Controllers And Data Processors Of Major Importance And All Matters Connected therewith NDPC/HQ/GN/VOL.03/B/24” < <https://ndpc.gov.ng/wp-content/uploads/2025/07/Updated-Guidance-Notice-on-Registration-2024.pdf>> accessed October 16, 2025.
- ^{viii} Ibid.
- ^{ix} Ibid.
- ^x Nigeria Data Protection Act 2023, Section 65.
- ^{xi} Ibid.
- ^{xii} Matthew Kosinki, “What is a data breach?” <[What Is a Data Breach? | IBM](#)> accessed October 16, 2025.
- ^{xiii} Nigeria Data Protection Act 2023, Section 65.
- ^{xiv} Ibid.
- ^{xv} Information Commissioners Office, “ Pseudonymisation” <[Pseudonymisation | ICO](#)> accessed October 16, 2025.
- ^{xvi} NDP Act 2023, General Application and Implementation directive 2025, Article 45
- ^{xvii} Muhammad Fasal Saittar and Anas Baig, “What is a Privacy Policy: A Complete Guide” (Secuirti, December 13, 2023) <https://securiti.ai/what-is-a-privacy-policy/> accessed October 16, 2025.
- ^{xviii} Section 24(2) of the Nigeria Data Protection Act 2023; Article 5 (1)(b) of the General Data Protection Regulation 2018, further stipulates that further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes
- ^{xix} Nigeria Data Protection Act 2023 Section 24(1)(c); the GDPR 2018 Article 5(1)(c).
- ^{xx} Nigeria Data Protection Act 2023 Section 24(1)(d); the GDPR 2018 Article 5(1)(d) ; Article 15 of the GAID 2025.
- ^{xxi} Nigeria Data Protection Act 2023 Section 24(1)(f) ; the GDPR 2018 Article 5(f) .
- ^{xxii} Nigeria Data Protection Act 2023 Section 24(1).
- ^{xxiii} Nigeria Data Protection Act 2023, Section 28
- ^{xxiv} GDPR.EU, “Cookies” < <https://gdpr.eu/cookies/> > accessed October 16, 2025.
- ^{xxv} European Data Protection Supervisor, “ Data Protection Officer” < https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en > accessed October 16, 2025.
- ^{xxvi} Nigeria Data Protection Act 2023, Section 28(1)
- ^{xxvii} Nigerian Data Protection Commission, “Definition and duties of a DPCO” < [DPCO Registration & Requirements – Nigeria Data Protection Commission](#)> accessed November 3, 2025.
- ^{xxviii} CookieYes, ‘Nigeria Data Protection Act (NDPA) 2023 – What You Need to Know’ <https://www.cookieyes.com/blog/nigeria-data-protection-act-ndpa/> accessed 26 November 2025.
- ^{xxix} Compos Mentis Legal Practitioners, ‘The Nigeria Data Protection Act 2023, Notable Provisions At A Glance’ (Mondaq, 7 April 2024) <https://www.mondaq.com/nigeria/privacy-protection/1433406/the-nigeria-data-protection-act-2023-notable-provisions-at-a-glance> accessed 26 November 2025
- ^{xxx} Nigeria Data Protection Act 2023, ss 1–2
- ^{xxxi} Nigeria Data Protection Act 2023, s 32
- ^{xxxii} Nigeria Data Protection Act 2023, s 4
- ^{xxxiii} LawPavilion, “NDP Act 2023 GAID 2025: A Comprehensive Guide to Nigeria’s New Data Protection Landscape” (LawPavilion Blog, 17 September 2025) <https://lawpavilion.com/blog/ndp-act-2023-gaid-2025-a-comprehensive-guide-to-nigerias-new-data-protection-landscape/> accessed 1 December 2025.
- ^{xxxiv} Nigerian Data Protection Commission, *Nigeria Data Protection Act – General Application and Implementation Directive 2025 (GAID)* art 7.
- ^{xxxv} CBN releases draft baseline standards for automated AML solutions, DataGuidance (21 May 2025) <https://www.dataguidance.com/news/nigeria-cbn-releases-draft-baseline-standards> accessed 1 December 2025.
- ^{xxxvi} *The procedure and requirements for obtaining a telecommunication licence in Nigeria*, Legal 500 (27 January 2025) <https://www.legal500.com/developments/thought-leadership/the-procedure-and-requirements-for-obtaining-a-telecommunication-license-in-nigeria/> accessed 1 December 2025.
- ^{xxxvii} DLA Piper, “Data Protection in Nigeria” <https://www.dlapiperdataprotection.com/index.html?c=NG&t=law> accessed 1 December 2025.

- xxxviii The Investment and Securities Act 2025 [https://home.sec.gov.ng/documents/1319/Investments and Securities Act 2025_x9rSXtl.pdf](https://home.sec.gov.ng/documents/1319/Investments%20and%20Securities%20Act%2025_x9rSXtl.pdf) accessed 26 November 2025.
- xxxix An Coimisun Chosaint Sonrai Data Protection Commission, “Principles of Data Protection” < <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection> > accessed November 18, 2025
- xl The Nigeria Data Protection Act 2023 Section 25(1)(a); a similar provision is made in The GDPR 2018 Article 6 (1)(a).
- xli The Nigeria Data Protection Act 2023 Section 25(1) (b)(i); a similar provision is made in The GDPR 2018 Article 6(1)(b).
- xlii The Nigeria Data Protection Act 2023 Section 25(1) (b)(ii); a similar provision is made in The GDPR 2018 Article 6(1)(c).
- xliii The Nigeria Data Protection Act 2023 Section 25(1)(b)(iii); a similar provision is made in The GPDR 2018Article 6(1)(d).
- xliv The Nigeria Data Protection Act 2023, Section 25(1)(b)(iv); a similar provision is made in The GDPR 2018, Article 6(1)(e).
- xlv The Nigeria Data Protection Act 2023, Section 25(1)(b)(v); a similar provision is made in The GDPR 2018, Article 6(1)(f).
- xlvi The Nigeria Data Protection Act 2023, Section 25(2)(a).
- xlvii The Nigeria Data Protection Act 2023, Section 25(2)(b).
- xlviii The Nigeria Data Protection Act 2023, Section 25(2)(c).
- lix The Nigeria Data Protection Act: General and Application and Implementation Directive 2025 in Schedule 1 (i) further explains that Fair means the data processing is free from prejudice and exploitation and it is generally consistent with civil liberties in a democratic society
- ⁱ IT Governance Europe, “GDPR: Understanding the 6 Data Protection Principles” (IT Governance Europe, June 6, 2024) < <https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles> > accessed July 26, 2025.
- ⁱⁱ The Nigeria Data Protection Act: General and Application and Implementation Directive 2025 in Schedule 1 (i)(iii) further defines transparency as the means of disclosure of all material facts that may help a data subject and the Commission to take informed decisions. Even where consent or contract is not the lawful basis relied upon for data processing, disclosure of material facts for the purposes of regulatory oversight is paramount.
- ⁱⁱⁱ Recital 58 of the General Data Protection Regulation 2018 < <https://gdpr-info.eu/recitals/no-58/> > accessed July 26, 2025.
- ⁱⁱⁱⁱ The Nigeria Data Protection Act 2023, Section 24(2); The General Data Protection Regulation 2018, Article 5 (1)(b), further stipulates that further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes
- ^{lv} The Nigeria Data Protection Act 2023, Section 24(1)(c); The GDPR 2018, Article 5(1)(c).
- ^{lv} Lauren Hendrickson, “Why Data Minimisation Is the Future of Privacy” (Identity, June 8, 2025) < <https://www.identity.com/why-data-minimisation-is-the-future-of-privacy/> > accessed November 20, 2025.
- ^{lvi} Ibid
- ^{lvii} Ibid
- ^{lviii} Lauren Hendrickson, “Why Data Minimisation Is the Future of Privacy” (Identity, June 8, 2025) < <https://www.identity.com/why-data-minimisation-is-the-future-of-privacy/> > accessed November 20, 2025.
- ^{lix} The Nigeria Data Protection Act 2023, Section 24(1)(d); The GDPR 2018, Article 5(1)(d); The NDPA GAID 2025, Article 15.
- ^{lx} Robert Healey, “The Data Privacy Principle of Storage Limitation” < <https://formiti.com/the-data-privacy-principle-of-storage-limitation-safeguarding-your-data> > accessed July 27, 2025.
- ^{lxi} The Nigeria Data Protection Act: General and Application and Implementation Directive 2025 in Schedule 8 (f) further describes “Accountability” to mean being: transparent; meticulous in keeping record of processing activities; promptly responsive to complaints and requests; promptly responsive to regulatory procedures and directives; and committed to the principles of data protection.
- ^{lxii} The Nigeria Data Protection Act 2023, Section 24(3).
- ^{lxiii} The GDPR 2018, Article 30.
- ^{lxiv} Information Governance Services, “What Does the GDPR Accountability Principle Ensure?” (Information Governance Services, January 7, 2025) < <https://www.informationgovernanceservices.com/articles/what-does-the-gdpr-accountability-principle-ensure/> > accessed July 27, 2025.
- ^{lxv} Ibid.
- ^{lxvi} Ibid.

- lxvii Ibid.
- lxviii The Nigeria Data Protection Act 2023, Section 28 of the
- lxix The Nigeria Data Protection Act 2023, Section 24(1)(f); The GDPR 2018 Article 5(f).
- lxx The Nigeria Data Protection Act 2023, Section 24(2).
- lxxi Nigeria Data Protection Act 2023, Section 24 (1) (d)
- lxxii Section 8.2 of the NDPR Implementation
- lxxiii NDPA General Application and Implementation Directive (GAID) 2025, Schedule 1, Paragraph 4(i)
- lxxiv Nigeria Data Protection Act 2023, Section 29 (1) (c)
- lxxv Nigeria Data Protection Act 2023, Section 39 (1)
- lxxvi Section 40(2) & (3) Nigeria Data Protection Act 2023.
- lxxvii Section 21, Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015, as amended by the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024
- lxxviii Nigerian Data Protection Act 2023, Section 41 (1)
- lxxix NDPA General Application and Implementation Directive (GAID) 2025, Schedule 5, Paragraph 1
- lxxx Nigerian Data Protection Act, 2023, Section 32
- lxxxi Information Commissioner's Officers, 'What is a Data Protection Impact Assessment' <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/>> Accessed on December 5, 2025
- lxxxii NDPA General Application and Implementation Directive (GAID) 2025, Article 7
- lxxxiii Nigerian Data Protection Act, 2023, Section 24 (f)
- lxxxiv See *Article 27 of the GAID* which states that "the provision of information to a data subject shall be in accordance with *Section 27 of the NDPA*. The information shall be clear and shall take into consideration vulnerable data subjects.
- lxxxv 'Data Subject Rights under the Nigeria Data Protection Act: Building an Effective Data Subject Rights Request Procedure' <<https://www.techhiveadvisory.africa/insights/data-subject-rights-under-the-nigeria-data-protection-act-building-an-effective-data-subject-rights-request-procedure>> accessed 25 July 2025
- lxxxvi Jyn Schultze-Melling, 'Data Subject Rights' in Ustaran E (ed), *European Data Protection: Law and Practice Book* (3rd edn, IAPP 2023) p.216
- lxxxvii In essence, it should be a format that is widely recognized format. The information contained therein should also be easily readable and not made with the intent to confuse or strain the data subject to read or understand.
- lxxxviii *Section 34(1)(b) of the NDPA.*
- lxxxix *Article 36(1) of the GAID and Section 24(1)(e) of the NDPA.*
- xc *Section 36(3) and (4).*
- xci *Section 34(1)(e) (i-iii) of the NDPA*
- xcii Jyn Schultze-Melling, 'Data Subject Rights' in Ustaran E (ed), *European Data Protection: Law and Practice Book* (3rd edn, IAPP 2023) p.223
- xciii *Section 38(2) of the NDPA.*
- xciv *Section 46 of the NDPA*
- xcv Ibid
- xcvi Article 28(3)(k) of the GAID
- xcvii Section 31(1) of the NDP Act
- xcviii The exceptions to the requirement for consent include: a) where processing is necessary to protect the vital interest of the child lacking capacity to consent, b) processing is carried out for the purpose of education, medical or social care and undertaken by professionals or similar service providers with a duty of confidentiality, c) processing is necessary for proceedings before a court relating to the child
- xcix Section 31(6) of the NDP Act
- c See Section 27 of the NDP Act
- ci Article 28 of the GAID
- cii Section 65 of the NDP Act
- ciii Section 30(1)(a) of the NDP Act
- civ The statutory exceptions as provided in Section 30 of the NDP Act include: a) processing for the purpose of performing the obligations of the data controller or exercising the rights of data subjects under employment laws, b) processing to protect the vital interest of data subjects who are physically or legally incapable of giving consent, c) processing carried out in the course of a NGO's legitimate activities with appropriate safeguards in place, d) processing for the conduct of legal proceedings, e) processing for reasons of substantial public interest. E.t.c
- cv Section 30(3) of the NDP Act
- cvi Section 41 of the NDP Act

-
- ^{cvii} Section 43 of the NDP Act. Note that the transfer may also be made if the transfer is necessary for important reasons of public interest, or required in the establishment, exercise and defense of legal claims.
- ^{cviii} Schedule 5 of the GAID which provides guidance on cross-border data transfer
- ^{cix} Section 24(1) of the NDP Act
- ^{cx} Schedule 1(4) of the GAID
- ^{cx i} Section 27(1)(e) of the NDP Act and Schedule 1(4)(vii) of the GAID
- ^{cx ii} Article 52 of the GAID, Data subject access request (DSAR) is a request directed to the organisation by a data subject, granting the data subject right to access information about personal data the organisation is processing.
- ^{cx iii} Article 41(9) of the GAID
- ^{cx iv} Section 40(1) of the NDPA
- ^{cx v} Section 40(1)(a) of the NDPA
- ^{cx vi} Section 40(1)(b) of the NDPA
- ^{cx vii} Section 40(3) of the NDPA
- ^{cx viii} Section 40(4), of the NDPA
- ^{cx ix} Section 40(8) of the NDPA
- ^{cx x} Section 46(1) of the Nigeria Data Protection Act, 2023
- ^{cx xi} Section 46(2) of the Nigeria Data Protection Act, 2023
- ^{cx xii} Section 47 of the Nigeria Data Protection Act, 2023
- ^{cx xiii} Section 47(2) of the Nigeria Data Protection Act, 2023
- ^{cx xiv} Section 48(1) of the Nigeria Data Protection Act, 2023
- ^{cx xv} Section 48(3)(4)(5) of the Nigeria Data Protection Act, 2023
- ^{cx xvi} Section 50 of the Nigeria Data Protection Act, 2023
- ^{cx xvii} Section 52 of the Nigeria Data Protection Act, 2023

CONTACT

LAGOS

KENNA Place
8, Ogunyemi Road, Palace Way, Oniru
PO Box 73002, Victoria Island, Lagos

ABUJA

1st Floor, Novare Central
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285, Abuja

ENUGU

3 Emmanuel Ngwu Street,
Old Emene Road, by AC Drug,
Thinkers Corner, Enugu.

+234 811 395 1052, +234 811 395 1053
legal@kennalp.com counsel@kennalp.com