Data Privacy Policy

Approved by:	Adebola Badmus
Role:	COO
Date:	1/6/2024

Revision history

Revision	Date	Description of Changes	Prepared By	Approved By
0.1	09/11/2023	Version 0.1	Project Team	

Distribution history

Revision	Date	Stakeholders

Control of hardcopy versions

The digital version of this document is the most recent version. The printed version of this manual is uncontrolled, and cannot be relied upon, except when formally issued by the **Document Controller** and provided with a document reference number and revision in the fields below:

Document Ref.		Rev.		Uncontrolled Copy	X	Controlled Copy	

Table of Contents

1. Introduction

This Data Privacy Policy outlines the commitment of Intelfort Nigeria Ltd ("we", "our", "us") to protecting the privacy and security of personal data processed on behalf of our clients. As a professional service provider in Data Management, Analytics, and AI, we act strictly as a data processor and not as a data controller, processing personal data only under the instruction of our clients in accordance with contractual, legal, and regulatory requirements.

---

2. Purpose of the Policy

The purpose of this policy is to:

- Ensure compliance with the General Data Protection Regulation (GDPR) and the Nigeria Data Protection Regulation (NDPR).
- Describe how we handle personal data, maintain data privacy, and meet security obligations.
- Provide transparency to clients, partners, and stakeholders on how data entrusted to us is protected.

---

3. Scope of the Policy

This policy applies to:

- All employees, contractors, and third parties who process data on behalf of Intelfort Nigeria Ltd.
- All data processing activities involving client-owned personal data.
- All systems, tools, applications, and services used in the delivery of our solutions and consultancy.

4. Definitions

For the purpose of this Data Privacy Policy, the following definitions apply in accordance with applicable data protection regulations, including the EU General Data Protection Regulation (GDPR) and the Nigeria Data Protection Regulation (NDPR):

Personal Data refers to any information relating to an identified or identifiable natural person (referred to as a "Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- a name, an identification number, location data, or an online identifier,
- or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

This includes but is not limited to personal names, addresses, phone numbers, email addresses, national identification numbers, IP addresses, biometric data, or any combination of data that can uniquely identify an individual.

Processing means any operation or sets of operations which is performed on personal data or on sets of personal data, whether or not by automated means. This includes but is not limited to:

- Collection
- Recording
- Organization
- Structuring

- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission
- Dissemination or otherwise making available
- Alignment or combination
- Restriction
- Erasure or destruction

As a data processor, our organization carries out processing activities solely on behalf of and under the instructions of the Data Controller.

Data Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

The Data Controller is responsible for ensuring that all data processing activities are compliant with applicable data protection laws, and for providing the legal basis on which personal data is processed. In the context of our services, our clients typically act as Data Controllers.

Data Processor refers to the natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller.

Our company, Intelfort Nigeria Ltd, acts as a Data Processor, performing data processing services strictly in accordance with the instructions of the Data Controller and in compliance with all applicable data protection laws. As a Data Processor, we do not determine the purposes or means of processing personal data.

Our processing responsibilities include, but are not limited to:

- Data integration and transformation
- Data storage and warehousing
- Reporting and visualizations
- Data quality enhancement
- Master data management
- Data analytics and artificial intelligence modeling

We implement appropriate technical and organizational measures to ensure the security and confidentiality of the personal data processed.

Data Subject means an identified or identifiable natural person whose personal data is processed. Data Subjects are the individuals to whom the personal data relates.

In our role as a Data Processor, we do not have a direct relationship with Data Subjects. Any inquiries or requests by Data Subjects, including rights of access, rectification, or deletion, should be directed to the Data Controller responsible for their data.

Sub-Processor refers to any third-party data processor engaged by our company who may have access to, or process, personal data on behalf of the Data Controller and under our instructions.

We ensure that all Sub-Processors are contractually bound to comply with data protection obligations that are no less protective than those set forth in our agreements with Data Controllers. Before engaging any Sub-Processor, we conduct due diligence to verify that the Sub-Processor implements adequate data protection and security measures.

We maintain a current list of all Sub-Processors upon request by any Data Controller and ensure transparency and accountability throughout the data processing chain.

---

5. Legal Basis for Processing Personal Data

As a data processor, we only process personal data on the instructions of our clients (the data controllers) and in accordance with:

- Article 28 of the GDPR
- Section 2.6 of the NDPR
- Relevant contractual agreements with our clients

---

6. Data Protection Principles

We uphold the following principles:

Lawfulness, Fairness, and Transparency

We process personal data lawfully and fairly, in a transparent manner that upholds the rights and interests of data subjects. This means:

- We only process personal data under a valid legal basis as defined by our clients (the Data Controllers), who ensure that data subjects have provided informed consent or that processing is otherwise legally justified.
- We support our clients in fulfilling their obligations to provide transparent disclosures to data subjects, in accordance with Articles 13 and 14 of the GDPR and Sections 2.1 and 2.2 of the NDPR.
- We ensure that our own processes, tools, and platforms are transparent, auditable, and support lawful use by our clients.

Purpose Limitation

We process personal data strictly for the purposes explicitly defined and documented by the Data Controller. Our systems and teams are designed to:

- Prevent unauthorized repurposing of data outside the scope of the Controller's instructions.
- Support clients in ensuring that any subsequent processing is compatible with the original purpose of collection.
- Maintain detailed processing records to demonstrate alignment with the agreed purposes.

Data Minimization

We encourage and implement the principle of data minimization by ensuring that:

- Only data that is adequate, relevant, and limited to what is necessary for the intended processing purpose is stored or processed.
- Our data ingestion and transformation pipelines are designed to filter out superfluous or unnecessary data fields where possible.
- We advise clients on best practices for minimizing the collection and retention of personally identifiable information (PII).

Accuracy

We support our clients in ensuring the personal data processed is accurate and, where necessary, kept up to date:

- We implement automated validation rules, deduplication algorithms, and enrichment services that promote data accuracy.
- Our Master Data Management (MDM) systems support consistent and synchronized data across multiple sources.
- We notify clients if we become aware of potentially inaccurate or outdated personal data during processing operations.

Storage Limitation

We do not retain personal data longer than necessary for the purposes of processing as instructed by the Data Controller:

- We provide configuration options and controls for data retention and deletion schedules.
- We support automated purging and archival mechanisms based on client-defined retention policies.
- All backups and archives containing personal data are maintained securely and only retained for durations aligned with contractual and regulatory requirements.

Integrity and Confidentiality

We ensure the security of personal data through the implementation of appropriate technical and organizational measures:

- Data is encrypted both at rest and in transit using industry-standard encryption protocols (e.g., AES-256, TLS 1.2+).
- Access to personal data is restricted based on the principle of least privilege and enforced through multi-factor authentication, role-based access control, and regular audits.
- We conduct periodic vulnerability assessments and penetration tests to proactively identify and remediate potential threats.
- All employees and subcontractors are subject to strict confidentiality agreements and undergo regular training on data protection and security practices.

Accountability

As a responsible Data Processor, we take full accountability for our data protection obligations and support our clients in meeting their own:

- We maintain detailed records of processing activities in line with Article 30 of the GDPR and Section 3.1(7) of the NDPR.
- We have implemented internal policies, training programs, and governance structures to uphold privacy compliance across all our services.

- We are prepared to assist Data Controllers with data protection impact assessments (DPIAs), audits, breach notifications, and the facilitation of data subject rights.

---

7. Roles and Responsibilities

- Clients (Data Controllers): Define processing requirements and ensure data subject rights.
- Intelfort Nigeria Ltd (Data Processor): Implements technical and organizational measures to ensure compliance.
- Data Protection Officer (DPO): Oversees data protection strategies and compliance efforts.

---

8. Categories of Personal Data Processed

We process a wide range of personal data as instructed by our clients, including:

- Biographical data (name, address, DOB)
- Contact data (email, phone)
- Financial data (transaction history, account details)
- Employment and academic records
- Health records (if applicable)

Note: Processing sensitive data is done under strict security protocols and legal basis.

---

9. Purposes of Data Processing

As a data processor, our processing activities are limited to:

- Data integration and migration
- Data cleansing and validation
- Data warehousing
- Advanced analytics and machine learning
- Reporting and dashboard development
- Master data management and data quality enhancement

---

10. Data Sharing and Third Parties

- Data is never shared or disclosed unless instructed by the controller.
- We do not sell, trade, or lease personal data.
- All third parties or sub-processors undergo strict due diligence and are bound by Data Processing Agreements (DPA).

---

11. International Data Transfers

- Where international data transfers occur (outside Nigeria or the EEA), we ensure:
- Compliance with Standard Contractual Clauses (SCCs) for GDPR.
- Compliance with NDPR Implementation Framework for Nigeria.
- Additional safeguards like encryption, anonymization, and audit logging.

---

12. Data Retention

- Personal data is only retained for the duration instructed by the client.
- Secure disposal processes are in place to delete or anonymize data at the end of its lifecycle.

---

13. Data Subject Rights

Data subject rights are enforced by the controller, but we cooperate fully in enabling them:

- Right to access, rectification, and erasure
- Right to restrict or object to processing
- Right to data portability
- Right to lodge a complaint

---

14. Security Measures

We implement a multi-layered security approach including:

- Encryption of data at rest and in transit
- Role-based access control (RBAC)
- Firewalls, intrusion detection systems, and anti-malware
- Regular security audits and penetration testing
- Secure software development lifecycle (SSDLC)

---

15. Data Breach Management

Any data breach is reported to the client within 24 hours of detection.

Breach logs, impact assessments, and mitigation strategies are documented.

We support the controller in notifying regulatory authorities and affected individuals if necessary.

---

16. Staff Training and Awareness

- All staff undergo annual Data Privacy and Security Training.
- Confidentiality agreements are signed at hiring.
- Awareness campaigns are conducted regularly to reinforce data protection culture.

---

17. Sub-processors and Third-Party Vendors

Sub-processors are selected after a due diligence assessment and are contractually obligated to comply with our privacy and security standards.

A current list of sub-processors is made available to clients upon request.

---

18. Monitoring and Review

Continuous monitoring of systems for vulnerabilities.

Internal audits are conducted at least annually.

The policy is reviewed every 12 months or upon regulatory changes.