MIRI AFRICA LIMITED

DATA PROTECTION AND PRIVACY GOVERNANCE POLICY

Policy Owner: (Privacy Officer / Data Protection Officer)

Approved By: Board of Directors

Effective Date: April 10, 2026

Review Cycle: Annually or upon material regulatory or operational change

1. POLICY STATEMENT

Miri Africa Limited ("Miri Africa" or the "Company") is committed to maintaining the highest standards of privacy, confidentiality, information governance, and data protection in the conduct of its business.

As a climate technology company that develops and deploys environmental monitoring systems, air quality tracking devices, connected technologies, software platforms, analytics tools, and related services, the Company processes personal data relating to customers, users, employees, contractors, suppliers, partners, regulators, and other stakeholders across multiple jurisdictions.

The Company recognises that personal data is a valuable asset and that the responsible handling of personal data is essential to maintaining trust, protecting individual rights, managing organisational risk, and complying with applicable legal and regulatory obligations.

This Policy establishes Miri Africa's enterprise-wide framework for the lawful, secure, transparent, and accountable processing of personal data and applies to all business activities, technologies, products, services, systems, and personnel involved in the processing of personal data.

The Company is committed to complying with applicable data protection laws, including:

- The Nigeria Data Protection Act 2023 (NDPA);
- The General Data Protection Regulation (EU) 2016/679 (GDPR);
- The UK GDPR;
- Applicable national data protection laws in jurisdictions where the Company operates; and
- Contractual obligations relating to privacy and data protection.

Compliance with this Policy is mandatory and forms part of the Company's broader corporate governance, risk management, information security, and regulatory compliance framework.

2. PURPOSE

The purpose of this Policy is to:

- establish a consistent framework for the processing of personal data;
- protect the rights and freedoms of individuals whose personal data is processed by the Company;
- define responsibilities and accountability for privacy and data protection;
- ensure compliance with applicable legal and regulatory requirements;
- minimise legal, operational, cybersecurity, financial, and reputational risks;
- support the responsible development and deployment of climate technology and environmental monitoring solutions; and
- promote a culture of privacy, accountability, and responsible data stewardship throughout the organisation.

3. SCOPE

This Policy applies to:

- all directors, officers, employees, consultants, contractors, interns, temporary staff, and agents of Miri Africa;
- all subsidiaries, affiliates, and business units controlled by Miri Africa;
- all personal data processed by or on behalf of the Company;
- all information systems, applications, devices, platforms, cloud services, and databases used by the Company; and
- all third parties processing personal data on behalf of the Company.

This Policy applies regardless of the format in which personal data is stored, including electronic, paper-based, audio, visual, biometric, or other formats.

4. DEFINITIONS

For the purposes of this Policy, the following terms shall have the meanings assigned to them below.

Anonymisation -The process of irreversibly altering data such that an individual can no longer be identified directly or indirectly from the information, whether alone or in combination with other information reasonably available to the Company or any third party. Information that has been properly anonymised is no longer considered personal data.

Consent - A freely given, specific, informed, and unambiguous indication of a data subject's wishes by which the data subject signifies agreement to the processing of personal data relating to them.

Customer Data - Any information, data, records, content, datasets, files, or materials provided to, collected by, or generated on behalf of a customer through the Company's products or services.

Customer Data may include personal data, environmental monitoring data, confidential information, or other data categories.

Data Controller - A natural or legal person, public authority, agency, or other body that determines the purposes and means of processing personal data.

Miri Africa acts as a controller where it determines why and how personal data is processed.

Data Processor - A natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller.

Miri Africa may act as a processor where it processes personal data solely on behalf of a customer, government agency, research institution, or other third party.

Data Protection Impact Assessment (DPIA) - A documented assessment process designed to identify, evaluate, and mitigate privacy and data protection risks associated with a proposed processing activity.

Data Subject - An identified or identifiable natural person to whom personal data relates.

An identifiable individual is one who can be identified directly or indirectly by reference to identifiers such as a name, identification number, location data, online identifier, or other factors specific to that individual.

Environmental Monitoring Data - Data generated through environmental monitoring systems, air quality sensors, climate adaptation technologies, weather monitoring equipment, connected devices, or related technologies.

Environmental Monitoring Data may include:

- air quality measurements;
- particulate matter readings;
- carbon dioxide measurements;
- temperature readings;
- humidity readings;
- atmospheric conditions;
- environmental risk indicators;
- environmental sensor outputs;
- climate monitoring information.

Environmental Monitoring Data is not necessarily personal data. However, where it can reasonably be linked to an identifiable individual, household, user account, employee, or other natural person, it shall be treated as personal data.

International Transfer - A transfer, disclosure, remote access, storage, or other processing of personal data outside the jurisdiction in which the personal data was originally collected.

Personal Data - Any information relating to an identified or identifiable natural person.

Personal data may include:

- names;
- email addresses;
- telephone numbers;
- identification numbers;
- location data;
- device identifiers;
- IP addresses;
- online identifiers;
- employment information; and
- any other information capable of identifying an individual directly or indirectly.

Personal Data Breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Personal data breaches may result from cyber incidents, human error, system failures, unauthorised disclosures, or other events compromising personal data.

Privacy by Design - The principle that privacy and data protection considerations should be integrated into the design, development, implementation, and operation of products, services, technologies, systems, and business processes.

Processing - Any operation or set of operations performed on personal data, whether by automated or non-automated means.

Processing includes:

- collection;
- recording;
- organisation;
- storage;
- adaptation;
- retrieval;
- consultation;

- use;
- disclosure;
- transmission;
- dissemination;
- restriction;
- erasure; and
- destruction.

Pseudonymisation - The processing of personal data in such a manner that the data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and subject to appropriate safeguards.

Pseudonymised data remains personal data.

Records of Processing Activities (ROPA) - The documentation maintained by the Company describing its personal data processing activities, including processing purposes, categories of personal data, categories of recipients, retention periods, security measures, and international transfers.

Sensitive Personal Data - Personal data requiring enhanced protection under applicable law.

Sensitive Personal Data may include information relating to:

- health;
- genetic data;
- biometric data;
- race or ethnic origin;
- religious or philosophical beliefs;
- trade union membership;
- sex life or sexual orientation;
- criminal convictions or offences; and
- other categories designated as sensitive under applicable law.

Sub-Processor - A third party engaged by a processor to process personal data on behalf of a controller.

Supervisory Authority - A regulatory authority responsible for monitoring compliance with applicable data protection laws, including the Nigeria Data Protection Commission and relevant European data protection authorities.

Derived Analytics – models, forecasts, insights, trends, scores, and outputs generated from raw environmental or customer data.

Telemetry Data – machine-generated operational information relating to device performance, diagnostics, connectivity, maintenance, and system health.

5. DATA PROTECTION PRINCIPLES

All processing of personal data by Miri Africa shall comply with the following principles:

Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly, and transparently.

Purpose Limitation

Personal data shall only be collected for specified, explicit, and legitimate purposes.

Data Minimisation

Only personal data that is necessary and proportionate to the relevant purpose shall be collected and processed.

Accuracy

Reasonable steps shall be taken to ensure personal data is accurate and up to date.

Storage Limitation

Personal data shall not be retained for longer than necessary.

Integrity and Confidentiality

Appropriate technical t and organisational measures shall be implemented to protect personal data.

Accountability

The Company shall be able to demonstrate compliance with applicable data protection obligations.

6. GOVERNANCE AND ACCOUNTABILITY

Board of Directors

The Board is responsible for oversight of privacy, data protection, and information governance risks and shall ensure that adequate resources are allocated to support compliance.

Chief Executive Officer

The CEO shall ensure that appropriate organisational measures are implemented to support compliance with this Policy.

Privacy Officer / Data Protection Officer

The Privacy Officer shall:

- monitor compliance;
- advise management;
- coordinate responses to data subject requests;
- oversee privacy impact assessments;
- coordinate regulatory engagement;
- support breach investigations;
- maintain records of processing activities.

Department Heads

Department heads shall ensure compliance within their areas of responsibility.

Employees and Contractors

All personnel are responsible for complying with this Policy and protecting personal data under their control.

7. Data Classification

The Company classifies information into the following categories:

Personal Data

Information relating to an identified or identifiable natural person.

Sensitive Personal Data

Personal data subject to heightened legal protection.

Customer Confidential Information

Information entrusted to the Company by customers or business partners.

Environmental Monitoring Data

Data generated through environmental monitoring systems, air quality sensors, climate adaptation devices, and related technologies.

Anonymised Data

Data that cannot reasonably be used to identify an individual.

Public Information

Information lawfully available to the public.

Appropriate security controls shall be applied based on classification.

8. Controller And Processor Activities

The Company may act as either:

Data Controller

Where Miri Africa determines the purposes and means of processing.

Examples include:

- employee management;
- website operations;
- customer relationship management;
- marketing activities.

Data Processor

Where Miri Africa processes personal data on behalf of a customer or partner.

Examples include:

- enterprise environmental monitoring deployments;
- municipal monitoring projects;
- research collaborations.

The Company shall identify its role before commencing any significant processing activity.

9. Lawful Basis For Processing

Personal data shall only be processed where an appropriate lawful basis exists, including:

- consent;
- contractual necessity;
- legal obligation;
- legitimate interests;
- vital interests; or
- public interest.

The lawful basis for each material processing activity shall be documented.

10. Data Subject Rights Management

The Company shall establish procedures for receiving, verifying, recording, assessing, and responding to requests relating to:

- access;
- rectification;
- erasure;

- restriction;
- portability;
- objection;
- withdrawal of consent;
- automated decision-making.

All requests shall be documented and managed within applicable legal timelines.

11. Records Of Processing Activities (ROPA)

The Company shall maintain records of processing activities in accordance with applicable legal requirements.

Such records shall include:

- categories of personal data;
- processing purposes;
- recipients;
- retention periods;
- international transfers;
- security measures.

12. Data Retention And Disposal

The Company shall maintain a Data Retention Schedule.

Personal data shall only be retained for as long as necessary for:

- operational purposes;
- legal compliance;
- contractual obligations;
- dispute resolution;
- risk management.

Upon expiry of retention periods, data shall be securely deleted, anonymised, or destroyed.

13. Third-Party And Vendor Management

Before engaging any processor or vendor that may access personal data, the Company shall undertake appropriate due diligence.

Requirements may include:

- privacy assessment;

- security assessment;
- contractual protections;
- execution of data processing agreements;
- international transfer assessments where applicable.

Vendor performance shall be monitored periodically.

14. International Data Transfers

Personal data shall not be transferred internationally unless:

- the transfer is lawful;
- appropriate safeguards are implemented; and
- required assessments have been completed.

The Company shall utilise mechanisms such as:

- adequacy decisions;
- Standard Contractual Clauses;
- UK transfer mechanisms;
- other recognised safeguards.

15. Privacy By Design And Data Protection Impact Assessments

Privacy considerations shall be incorporated into the design and development of products, technologies, services, and business processes.

A Data Protection Impact Assessment (DPIA) shall be conducted where processing is likely to result in a high risk to the rights and freedoms of individuals.

DPIAs shall generally be required for:

- large-scale monitoring activities;
- location-based monitoring;
- new sensor deployments;
- artificial intelligence or automated decision-making systems;
- large-scale analytics initiatives;
- processing involving vulnerable groups.

16. Environmental Data Governance

Given the Company's climate technology operations, special consideration shall be given to environmental monitoring data.

The Company shall maintain clear distinctions between:

- personal data;
- customer-owned data;
- environmental monitoring data;
- anonymised datasets;
- derived analytics and models.

Environmental data shall be processed in accordance with applicable contractual, legal, and governance requirements.

17. Information Security Requirements

Appropriate technical and organisational measures shall be implemented including:

- encryption;
- access controls;
- authentication mechanisms;
- vulnerability management;
- monitoring and logging;
- business continuity measures;
- physical security controls.

The Company's Information Security Policy shall operate alongside this Policy.

18. Incident Response And Breach Management

All personnel shall immediately report suspected privacy incidents, security events, or personal data breaches. The Company shall maintain documented procedures for:

- incident reporting;
- investigation;
- containment;
- recovery;
- notification;
- post-incident review.

All incidents shall be documented and reviewed.

19. Training And Awareness

All personnel shall receive privacy and data protection training appropriate to their role.

Training shall include:

- onboarding training;
- annual refresher training;
- specialised role-based training where required.

Training records shall be maintained.

20. Monitoring, Audit And Compliance Review

The Company may conduct:

- internal audits;
- compliance reviews;
- processor audits;
- risk assessments;
- policy effectiveness reviews.

Findings shall be reported to management and corrective actions implemented where necessary.

21. Non-Compliance

Failure to comply with this Policy may result in:

- disciplinary action;
- suspension of access privileges;
- contractual remedies;
- termination of employment or engagement; and
- legal or regulatory action where appropriate.

22. Policy Review

This Policy shall be reviewed at least annually and whenever there are significant changes in:

- applicable law;
- business operations;
- technologies;
- processing activities; or
- organisational structure.

Approved revisions shall be communicated to relevant personnel.