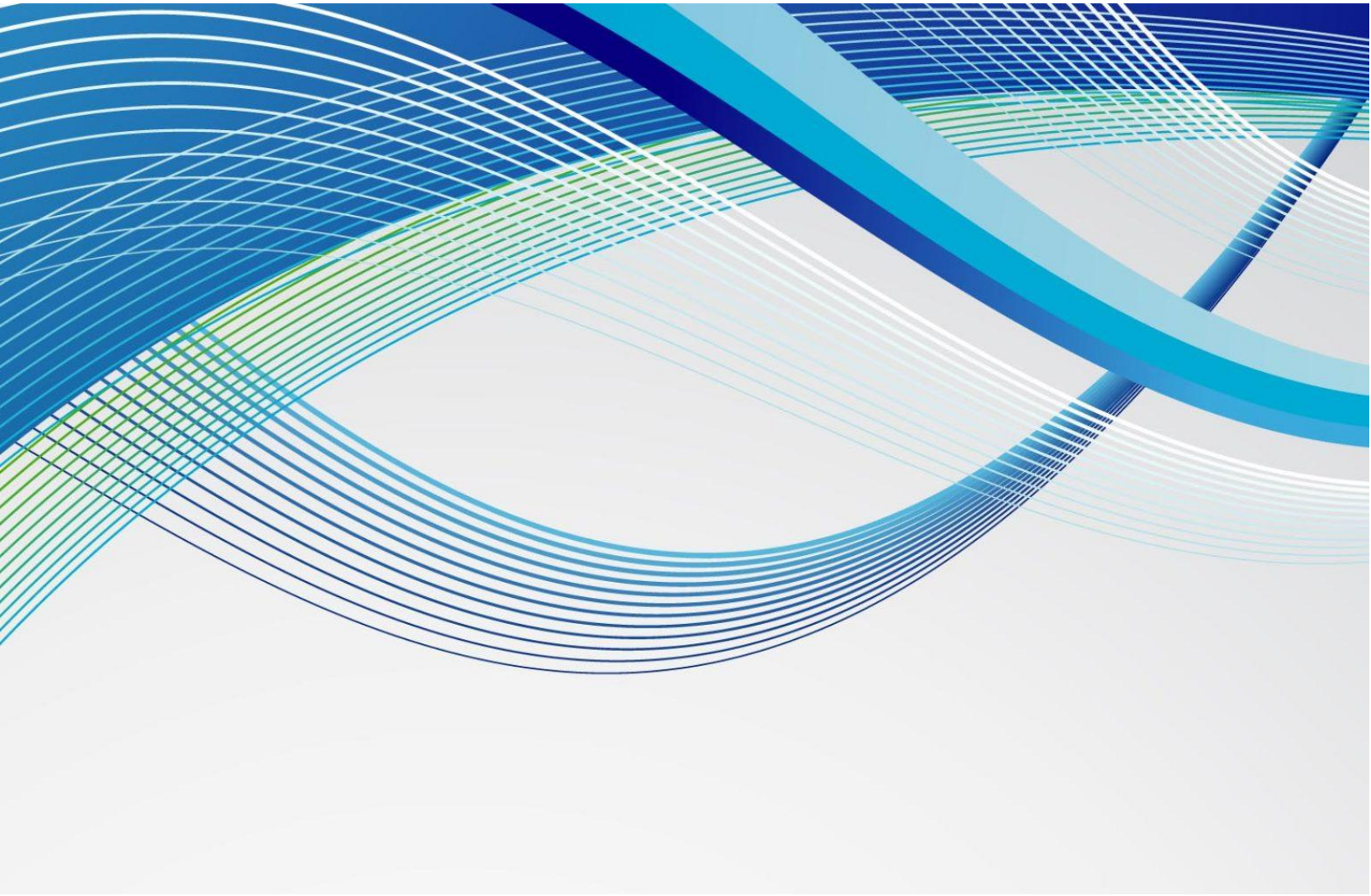
M31 RESEARCH
Evidence · Insight · Impact

CLASSIFICATION
Public



M31 RESEARCH • POLICY DOCUMENT

DATA PROTECTION AND CONFIDENTIALITY POLICY

M31 Research's commitment to protecting personal data and safeguarding confidential information

DOCUMENT REF.	VERSION	Updated
POL-001	V3.0	22 Jun 2026

Document Summary

Field	Detail
Policy title	Data Protection and Confidentiality Policy
Document reference	POL-001
Version	v1.0
Effective date	1 Feb 2021
Classification	Public

Contents

1. Purpose

This policy sets out M31 Research's commitment to protecting the personal data and confidential information it collects, holds, and processes in the course of its research and operations. It exists to ensure compliance with applicable data protection laws and client requirements, to protect the rights and privacy of research participants, staff, and partners, and to maintain the trust placed in us as a research organisation.

2. Scope

This policy applies to all personal and confidential data processed by M31 Research, in any format, across all projects and countries in which we operate. The table below summarises who and what it covers.

Applies to	Does not apply to
All M31 Research employees, associates, consultants, enumerators and field teams, interns, and volunteers, and all personal and confidential data processed by M31 Research in any format.	**Fully anonymised or aggregate data that cannot identify an individual. Third-party processors are covered through data processing agreements that require equivalent standards.**

3. Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person (the data subject).
Sensitive (special category) data	Personal data revealing health, ethnicity, religion, sexual orientation, political opinions, or biometric and genetic data, which requires additional protection.
Data subject	The individual to whom personal data relates, including research participants and staff.
Processing	Any operation performed on data, such as collection, recording, storage, use, sharing, or deletion.
Data controller	The party that determines the purposes and means of processing personal data.
Data processor	The party that processes personal data on behalf of a controller.
Confidential information	Non-public information, including client, project, commercial, and proprietary information, that must be protected from unauthorised disclosure.

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

4. Policy Statement

M31 Research is committed to the following principles:

- **Process personal data lawfully, fairly, and transparently, and only for specified, legitimate purposes.**
- **Collect only the minimum data necessary, and retain it only for as long as required.**
- **Obtain valid, informed consent from research participants and respect their right to withdraw.**
- **Keep personal and confidential data accurate, secure, and protected by appropriate technical and organisational measures.**
- **Apply heightened protection to sensitive (special category) personal data.**
- **Anonymise or pseudonymise data wherever possible, particularly for analysis and reporting.**
- **Restrict access to data on a need-to-know basis and protect confidential information from unauthorised disclosure.**
- **Transfer data securely and only under appropriate agreements and safeguards, including for cross-border transfers.**
- **Uphold data subjects' rights to access, correct, and request deletion of their data.**
- **Report and manage personal data breaches promptly.**

5. Roles & Responsibilities

Role	Responsibility
Leadership / Board	Accountable for this policy. Ensures the resources and culture needed for data protection compliance, and reviews performance.
Policy Owner	The Managing Director owns and maintains this policy, ensures compliance across projects and operations, and reports to the Board.
Managers	Project leads and managers ensure project-level compliance, consent procedures, and secure storage, and brief their teams.
All Staff	Handle data securely, follow consent and confidentiality rules, report breaches promptly, and complete required training.
Data Protection Focal Point	Advises on data protection compliance, maintains records of processing, and coordinates breach response and data protection impact assessments.

6. Procedures

1. **Define the lawful basis and purpose for collecting personal data at the design stage of each project.**
2. **Obtain and document informed consent from research participants before data collection.**
3. **Collect only necessary data and store it securely, using encryption, access controls, and secure devices.**
4. **Anonymise or pseudonymise data for analysis and reporting wherever feasible.**
5. **Restrict access to personal and confidential data on a need-to-know basis.**
6. **Share or transfer data only under approved data sharing or processing agreements and through secure channels.**
7. **Apply agreed retention periods and securely delete or destroy data when it is no longer required.**
8. **Respond to data subject requests for access, correction, or deletion within applicable timeframes.**
9. **Report any suspected or actual data breach immediately to the Data Protection Focal Point, who will contain, assess, notify, and remediate as required.**
10. **Provide data protection and confidentiality training to all staff and field teams.**

7. Compliance & Monitoring

Compliance with this policy is mandatory. M31 Research will monitor adherence through:

- **maintenance of records of processing and of data sharing and processing agreements;**
- **the inclusion of data protection checks in project quality and inception reviews;**
- **periodic audits of data security, storage, and retention;**
- **logging and review of data breaches, data subject requests, and corrective actions.**
- Breaches may result in disciplinary action up to and including termination of employment or contract, and, where relevant, referral to the responsible data protection authority. Individuals and the organisation may also face legal liability.

8. Related Documents

- **M31 Research Information Security Policy**
- **M31 Research Research Ethics Policy**
- **M31 Research Safeguarding Policy**
- **M31 Research Records Management and Retention Policy**
- **M31 Research Social & Environmental Management Policy**

- **Zambia Data Protection Act No. 3 of 2021, and equivalent data protection legislation in other countries of operation**
- **EU General Data Protection Regulation (GDPR), where applicable**
- **Client and donor data protection and confidentiality requirements**

9. Review

This policy will be reviewed every 12 months, or sooner if circumstances change, such as new legislation, revised client or donor requirements, or significant changes to M31 Research's operations.

10. Contact

Questions about this policy?
Owner: M31 Research
Email: info@m31r.com
Phone: +260978937745