MIC Global Risks Insurance Brokers (Uganda) Limited

Data Protection Policy

Contents

NOTICE

This policy document is the property of MIC Global Risks Insurance Brokers (Uganda) Limited and describes the IT equipment and facilities management as applied to the operations of the company. Reproduction of this manual, in part or as a whole, is not permitted without the authorization of the Head of IT.

The information contained in this policy document may not be divulged or used for any other purpose other than that intended. The procedures described and related documentation shall not be regarded as legally binding upon the Company.

The right is reserved to amend the contents of this policy document and the procedures referred to therein to reflect any changes to circumstances, methods or products which may apply from time to time.

1. Introduction

1.1. Data Protection Policy

This is the original version of the Data Protection Policy . Any revisions to this policy shall be denoted by the appropriate version numbers and the effective revision dates.

1.1.1. Document Revision History

DOCUMENT'S REVIEW RECORD		
DOCUMENT NAME	Version	EFFECTIVE DATE
Data Protection Policy	Version 1.0	09/07/2024

1.2. Policy updates and review

- Revisions to this policy shall be initiated by the business needs in line with regulatory requirements on Data Protection or shall be put for review to the Board of Directors biennially.
- The revisions to the Policy shall be deemed necessary to ensure compliance with any changes to the laws governing Data Protection.
- The IT Policy team will be responsible for ensuring the policy is regularly reviewed and the timeframe for review is appropriate to facilitate efficient review of the policy against the operations of the Company.
- Review dates shall be assigned by the IT Policy Team in consultation with the Senior Management and Stakeholders.
- The Senior Management and Stakeholders shall ensure that:
- Any revisions to the policy shall be compliant with the prevailing laws on Data Protection.
- That in line with the purpose and goals of the policy, the revisions remain consistent in relation to the Company's overall strategic plan.
- That any associated policies are modified, suspended or archived accordingly.
- That after every review, there is an implementation plan for communication and training of

employees to guarantee compliance with the revised provisions of this policy.

- The IT Policy team shall ensure that MIC Global Risks Insurance Brokers (Uganda) Limited implements a policy development process to maintain a continuous improvement cycle in respect of this policy.

1.3. Purpose

The purpose of this document is to describe **MIC Global Risks Insurance Brokers (Uganda) Ltd** responsibilities regarding the protection of personal data.

1.4. Principles of Processing of Personal Data

MIC Global Risks Insurance Brokers (Uganda) Ltd has adopted the following principles to govern its collection, processing, use, retention, transfer, disclosure, and destruction of Personal Data:

PRINCIPLE	DEFINITION
Right to privacy	Personal Data shall be processed in accordance with the right privacy of the Data Subject.
Lawfulness, Fairness and Transparency	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. MIC shall inform the Data Subject the Processing which will occur, through Terms and Conditions (transparency). The Processing shall match the description given to the Data Subject (fairness), and it shall be for one of the purposes specified in the applicable Data Protection regulations (lawfulness).
Purpose Limitation	Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means MIC shall specify exactly what the personal data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.
Data Minimization	Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed. This means MIC shall not store any Personal data beyond what is strictly required.
Accuracy	Personal Data shall be accurate and kept up to date. This means MIC shall have in place processes for identifying and addressing out-of-date, incorrect, and redundant Personal Data.
Storage Limitation	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed, in line with legal and regulatory requirements. This means MIC shall, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Integrity & Confidentiality	Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including reasonable protection against unauthorized or unlawful Processing, and against accidental loss, destruction, or damage. MIC shall use appropriate technical and organizational measures to ensure the integrity and confidentiality of Personal Data are always maintained.
Valid explanation	A valid explanation shall be provided to a Data Subject whenever information relating to family or private affairs is required.
Transfer out of Uganda	Personal Data shall only be transferred out of Uganda if there are adequate data protection safeguards in place or if there is consent from the Data Subject.

1.5. Scope

This policy applies to:

- All clients Personal Data.
- All staff of MIC Global Risks Insurance Brokers (Uganda) Ltd.
- All third parties who are contracted to collect, use, retain, transfer, disclose, store and destroy customer and staff Personal Data belonging MIC Global Risks Insurance Brokers (Uganda) Ltd.
- All MIC Global Risks Insurance Brokers (Uganda) Ltd locations where a data subject's Personal Data is processed, collected, retained, transferred, disclosed, stored and destroyed in the context of the business activities and/or for the provision or offer of services to individuals.

1.6. Policy

1.6.1. Policy Dissemination and Enforcement

Senior management of MIC Global Risks Insurance Brokers (Uganda) Ltd shall ensure that all its employees are aware of and shall comply with the contents of this policy. In addition, MIC Global Risks Insurance Brokers (Uganda) Ltd shall make sure all Third Parties engaged to process Personal Data on its behalf (i.e., their Data Processors) are aware of and comply with the contents of this policy. Commitment to such compliance shall be obtained from all Third Parties (in written form, via clauses or contractual obligations), whether companies or individuals, prior to granting them access to Personal Data controlled by MIC Global Risks Insurance Brokers (Uganda) Ltd.

1.6.2. Data Protection By design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them shall go through a risk assessment followed by an approval process based on the risk assessment results before commencement.

In liaison with the data protection officer or designated personnel, each process owner shall ensure that a Data Protection Impact Assessment (DPIA) is conducted proactively for all new or enhancement of existing technology, innovation, process, or product that falls within their scope of responsibility. The DPIA carried out shall envisage processing operations on the protection of Personal Data prior to Personal Data processing where a data processing operation is likely to result in a high risk to the rights and freedoms of a Data Subjects by virtue of its nature, scope, context, and purposes.

1.6.3. External Compliance reviews

To confirm that an adequate level of compliance is being achieved in relation to this policy, the Board may call for an external data protection compliance audit. The scope of the compliance audit will include the following.

- Assignment of responsibilities
- Raising awareness
- Training of Employees
- Adequacy of organizational and technical controls to protect Personal Data
- Records management procedures (including data minimization)
- Adherence to the qualified rights of the Data Subject
- Privacy by Design and Default
- Express Consent
- Personal Data transfers
- Personal Data incident management (including Personal data breaches)
- Personal Data complaints handling
- Currency of Data Protection policies and Privacy Notices
- Accuracy of Personal Data being stored
- Conformity of Data Processor activities
- Adequacy of procedures for redressing poor compliance.

1.7. Record Keeping

Personal Data shall only be retained for as long as it is reasonably necessary to satisfy the purpose for which it is processed unless the retention is:

- Required or authorized by law.
- Reasonably necessary for a lawful purpose; and
- Authorized or consented by the Data Subject.

1.8. Direct Marketing

MIC Global Risks Insurance Brokers (Uganda) Ltd shall not provide, use, obtain, procure Personal Data of a Data Subject for the purpose of direct marketing without prior consent of the Data Subject. This includes profiling of the Data Subject for the said purpose.
MIC Global Risks Insurance Brokers (Uganda) Ltd shall provide means for clients to easily 'opt out' of direct marketing emails/communication, e.g., by physical and electronic means.

1.9. Independent Assurance

The Internal Audit department shall independently evaluate the adequacy of implementation of this policy.

1.10. Rights of a Data Subject

A Data Subject has the following rights:

- Right to be informed of the use to which their Personal Data is to be put.
- Right to access their Personal Data in custody of Data Controller or Data Processor.
- Right to object to the collection or processing of all or part of their Personal Data.
- Right to correction and/or deletion of false or misleading data about them.
- Right to portability.

- Right to erasure.
- Right to object to direct marketing.
- Right to withdraw consent.

1.11. Data Collection, Retention & Transfer

MIC Global Risks Insurance Brokers (Uganda) Ltd shall not process Personal Data unless one of the following applies:

- The Data Subject consents to the processing for one or more specified purposes.
- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- For the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject before entering a contract.
- For compliance with any legal obligation to which MIC Global Risks Insurance Brokers (Uganda) Ltd is subject.
- Where the MIC Global Risks Insurance Brokers (Uganda) Ltd has given proof to the relevant authorities on the appropriate safeguards with respect to the security and protection of Personal Data, including jurisdictions with commensurate data protection laws.
- To protect the vital interests of the Data Subject or another person.
- For the performance of a task carried out in the public interest or in the exercise of official authority vested in MIC Global Risks Insurance Brokers (Uganda) Ltd.
- For the legitimate interests pursued by MIC Global Risks Insurance Brokers (Uganda) Ltd or the Data Processor by a Third Party to whom the data is disclosed, except if the processing is unwarranted in any case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the Data Subject.
- The collection is to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.
- If Personal Data is collected from someone other than the Data Subject, the Data Subject shall be informed of the collection unless one of the following apply:
- the Data Subject has received the required information by other means;
- the information shall remain confidential due to a professional secrecy obligation;
- A national law expressly provides for the collection, Processing, or transfer of the Personal Data; or
- Where it has been determined that notification to a Data Subject is required, notification shall occur promptly, but in no case later than one month unless otherwise stated by applicable laws or regulations.

In addition, MIC Global Risks Insurance Brokers (Uganda) Ltd shall ensure that;

- It registers as a Data Controller and Data Processor with the Personal Data Protection
- Office and maintain a registration certificate.
- It maintains a register of Systems which shall be reviewed at least annually, for data types stored, and how these are secured and processed.
- It determines the lawful basis of collecting/processing of this data.
- It considers data requests from its clients that are within the confines of applicable laws.
- All data processed by MIC Global Risks Insurance Brokers (Uganda) Ltd shall be done on one of the following lawful bases:
    - Consent.
    - Contract.
    - Legal obligation; or
    - Legitimate interests under approval of regulatory body.

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall securely kept with the personal data. Further where communications are sent to individuals based on their consent, the option for the individual to revoke their consent shall be clearly available and systems shall be in place to ensure such revocation is reflected accurately in MIC Global Risks Insurance Brokers (Uganda) Ltd systems.

- All Personal Data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Reasonable steps are taken to ensure Personal Data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that Personal Data is kept up to date.
- All Personal Data is not kept for longer than necessary, in this regard, MIC Global Risks Insurance Brokers (Uganda) Ltd shall put in place archiving guidelines for each area in which Personal Data is processed. The archiving guidelines shall consider what data should/shall be retained, for how long, and why.
- All Access to Personal Data is limited to personnel who need access and appropriate security shall be in place to avoid unauthorized sharing of information.
- Where Personal Data is deleted, that this is done in a manner that the Personal Data is irrecoverable.

1.12. Third Party data protection requirements

Before entering into any third-party relationships, MIC Global Risks Insurance Brokers (Uganda) Ltd shall take deliberate steps to conduct an assessment of risk related to the vendor relationship, understand the compliance, reputational, strategic, operational, and transactional risks relating to a particular vendor before entering into a contractual relationship.

Any third party who has access to MIC Global Risks Insurance Brokers (Uganda) Ltd's data classified as Personal Data or confidential information shall be expected to demonstrate their security policies, processes, and procedures and prove that they are able to provide adequate protection of such data, including against misuse or compromise. At a minimum the vendor shall ensure the following.

REQUIREMENTS	MANDATORY MEASURES
Organization of Information Security	Have in place documented policies and measures appropriate to prevent any access to Confidential Information and comply with and meet all applicable Information Security best practices standards and guidelines.
Compliance and Accreditation	Be compliant with all applicable laws and regulations. Conducts regular audits/evaluation of its governance internal controls, its financial reporting and a SOC2 report, evidencing the Third-Party's ability to securely manage MIC Global Risks Insurance Brokers (Uganda) Ltd's data. The SOC2 report presented should include the following; Relevant Aspects of the Control Environment (including Organizational Structure and Assignment of Authority and Responsibility), Risk Assessment Process, Information and Communication Systems, and Monitoring; Security procedures and policies in place/adequacy; Physical Security and logical security measures; and Monitoring (Vulnerability Scanning and Monitoring, Penetration Testing and vulnerability scanning)
Business Continuity Management and	Shall develop, operate, manage, and revise business continuity and disaster recovery (BCP/DR) plans. Such plans shall include BCP/DR roles and

Disaster Recovery	responsibilities, established recovery time objectives and recovery point objectives, daily back-up of data and systems, off-site storage of backup media and records, record protection and contingency plans commensurate with the requirements of MIC Global Risks Insurance Brokers (Uganda) Ltd. Shall have documented procedures for the secure backup and recovery of MIC Global Risks Insurance Brokers (Uganda) Ltd's Personal Data or higher, which shall include, at a minimum, procedures for the transport, storage, and disposal of the backup copies of the data and, upon MIC Global Risks Insurance Brokers (Uganda) Ltd request, provide such documented procedures.

1.13. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, or there is reasonable ground to believe Personal Data has been accessed or acquired by an unauthorized person, the breach shall be investigated and reported within the prescribed period to the Personal Data Protection Office. MIC Global Risks Insurance Brokers (Uganda) Ltd shall also communicate the breach to the Data Subject in the prescribed manner unless the identity of the Data Subject cannot be established.

2. ROLES & RESPONSIBILITIES

2.1. Data protection Officer (DPO)

The DPO shall:

- Ensure that MIC Global Risks Insurance Brokers (Uganda) Ltd 's IT systems and records management procedures comply with all relevant data privacy and protection law, regulation and policy (including in relation to the retention and destruction of data).
- Collaborate with the Information Security office to maintain records of all data assets and exports and maintaining a data security incident management plan to ensure timely remediation of incidents including impact assessments, security breach response, complaints, claims or notifications.
- Implement measures and the privacy policy to manage data use in compliance with the local and international laws, including assisting in vendor management reviews.

- Work with key internal stakeholders in the review of projects and related data to ensure compliance with local data privacy laws, and where necessary, complete and advise on privacy impact assessments.
- Serve as the primary point of contact and liaison for the Personal Data Protection Office on all data protection related matters.
- Review vendor contracts and consents in liaison with the legal department.
- Monitor changes to local privacy laws and making recommendations to the BOD when appropriate.
- Coordinate and conduct data privacy audits.
- Collaborate with the Information Security department to raise employee awareness of data privacy and security issues and providing training on the subject matter.

3. Related policies, standards and guidelines

This policy is aligned to the following laws, regulations, and guidelines:

- Data Protection and Privacy Act 2019
- General Data Protection Regulation (GDPR).

The above shall be read together with the following polices.

- Information Technology Security Policy
- Incident Management Policy

4. Terms and definitions

Personal Data - Any information (including opinions and intentions) relating to an identified or identifiable natural person ('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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Sensitive Personal Data - Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Subject - Any living individual who is the subject of Personal Data held by an organization. Examples for MIC Global Risks Insurance Brokers (Uganda) Ltd include potential staff and clients, current staff and clients, former staff and clients, consultants, and contractors etc.

Data Owner - Natural or legal person, public authority, agency, or other body having legal rights and complete control over a single piece or set of data elements. The data owner defines and provides information about data assets including the acquisition, use and distribution policy of said data.

Data Controller -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.

Data Processor - Natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Data Controller.

Employees- All natural or legal persons having a direct employment contract with MIC Global Risks Insurance Brokers (Uganda) Ltd.

Personal Data Protection and Privacy Act, 2019 - A regulation to protect the privacy for all individuals personal data within Uganda by regulating the collection and processing of personal information, to provide for the rights of the persons whose data is collected and the obligations of the data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and for related matters.

Third Parties - A natural or legal person, public authority, agency, or body other than the Data Subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process Personal Data on behalf of MIC Global Risks Insurance Brokers (Uganda) Ltd.

Vendor -A natural or legal person that provides goods or services to MIC Global Risks Insurance Brokers (Uganda) Ltd to support the running of MIC Global Risks Insurance Brokers (Uganda) Ltd's operations.

Consultant - Expert or professionals in a specific field, with a wide area of knowledge in a specific subject, assisting MIC Global Risks Insurance Brokers (Uganda) Ltd in optimization of its business processes and providing objective advice, expertise, and specialist competencies which the organisation needs to achieve its business objectives.

Direct marketing - The communication of any advertising or marketing material that is directed at any individual.

General Data Protection Regulation (GDPR) - A regulation in European Law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EAA). It also addresses the export of Personal Data outside the EU and EEA areas.

Processing - Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated means, such as 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.

Profiling - Any form of automated processing of Personal Data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the Data Subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the individual.

Personal Data Breach - An event leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data Subject Consent - Any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data.

Removable Media - Any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, diskettes, and USB drives. Removable media simplifies moving of data.

Filing system - Any structured set of Personal Data, which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

5. Enforcement

Failure to comply with the provisions of this policy shall be subject to HR established disciplinary actions, including but not limited to suspension, summary dismissal, and/or termination of employment or contract in accordance with HR disciplinary procedures in place.

Such violations may also extend a personal liability on the parties involved in line with provisions of the relevant legislation.

Third parties found to be in breach of the provisions of this policy shall be subject to relevant penalties or contract termination as shall be prescribed by the third-party contracts.

6. Document control panel

DOCUMENT CONTROL PANEL			
FILE NUMBER		MICUG-DPP-Ver -1.0	
OWNER		IT Department MIC Global Risks Insurance Brokers (Uganda) Limited	
HISTORY			
Date	Author Name	Changes	Approver
09/07/2024	AKK	Original Data Protection Policy development and Adoption	As per Section 7