EAST AFRICA REINSURANCE COMPANY LIMITED

DATA PRIVACY NOTICE

April 2023

Table of Contents

DATA PRIVACY NOTICE

This data privacy notice describes how East Africa Reinsurance Company Limited (the "Company") processes and uses personal data collected from you in the normal course of business. The Company is committed to protecting and respecting your privacy by processing your personal data lawfully, fairly and in a transparent manner and in compliance with Data Protection Act, 2019 (KDPA) and associated regulations.

1. Who we are

East Africa Reinsurance Company Limited is a leading regional reinsurer headquartered in Nairobi, Kenya. We offer both short-term and long-term reinsurance solutions to insurance companies locally and regionally, mainly in Sub-Saharan Africa. We seek to add value to our clients' businesses by being responsive, agile and flexible with respect to their reinsurance needs.

2. Scope

This data privacy notice applies to all natural persons whose personal data is collected and processed by the Company in the normal course of our business. The Company collects and processes personal data relating to:

- Stakeholders of our corporate customers and business partners:
  - Including shareholders (owners), directors and senior management team
- Beneficiaries of insurance contracts under our reinsurance programs:
  - Including ultimate policyholders, claimants or beneficiaries of the underlying insurance policies.
- Stakeholders of our service providers (suppliers, consultants, contractors, etc.):
  - Including business owners, proprietors, directors and management team.
- Any other third parties that may enter into a business relationship with us.

3. Personal data collected and processed by us

For the purposes of this data privacy notice, *"personal data"* refers to any information relating to an identified or identifiable natural person while a *"data subject"* means an identified or identifiable natural person who is the subject of personal data.

A data subject can be identified from the data collected directly from them, through our clients and intermediaries or their authorized agents or when that data is taken together with other information that the Company may come into possession. The table below highlights the type and nature of personal data that we may collect from you (as the data subject) depending on your relationship with us:

Information Type	Examples of personal data collected
Personal identification information	Name, telephone number, email address, postal address, physical address, etc.
Government generated information	National Identification Number (ID), Tax PIN and Registration Certificates, Passport Number, NSSF/NHIF numbers, etc.
Financial information	Bank account details, investments, etc.
Sensitive personal information	Date of birth, age, gender, race, marital status, dependents, etc.
Employment and education information	Employment history, educational background, professional membership, etc.
Medical information	Health status, previous and current ailments, injury or disability information, etc.

Audio-visual information	Photographs, videos, telephone recordings, etc.

4. Collecting your personal data

We collect and use your personal data to carry out designated business activities. As a customer (or a third party service provider), you are obligated to provide certain personal data to us that are pertinent to the specific business transaction involved, pursuant to applicable legal, contractual and regulatory requirements and obligations.

Personal data provided by you mainly enables us to verify your identity and to fulfill our contractual obligations depending on the nature of our relationship with you.

We obtain personal data about you, directly or indirectly, from sources such as:

- Know Your Client (KYC) forms completed by you, your authorized representative or your service provider to facilitate our Customer Due Diligence (CDD) procedures;
- Contractual agreements and other on-boarding documents completed by you or your authorized representatives to formalize our business relationship;
- Meetings (physical/virtual), telephone or email conversations and other forms of communication between us in the normal course of business and execution of contractual arrangements;
- Interactions between you and us through our social media platforms or our website (www.eastafricare.com);
- Communications between us and intermediaries or agents (e.g. insurance/reinsurance brokers) who act on your behalf; or
- Publicly available information about you that can be found on your website, daily newspapers, or other public social media platforms.

5. Use of your personal data

The purposes for which we use your personal data differs depending on the nature of our relationship with you and communications between us. In general however, we will collect, use and process your personal data to:

- Perform or fulfil our legal and financial obligations under various contractual arrangements (e.g. under the reinsurance contracts, service contracts, etc.) such as processing claims, settling bills, reconciling balances, resolving conflicts, etc.;
- Comply with applicable laws and regulations that obligate us to collect and process specified personal data, such as:
    - Collecting specified personal data from business counterparties in line with regulatory guidelines on Know Your Client (KYC), Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT);
    - Submitting specified personal data through periodic returns to relevant regulatory bodies such as Insurance Regulatory Authority (IRA), Financial Reporting Center (FRC), Kenya Revenue Authority (KRA) and Retirements Benefits Authority (RBA), among others; and
    - Complying with the various law enforcement agencies in the event of legal proceedings or in compliance with court orders.
- Carryout requisite customer due diligence and perform appropriate risk assessment to either detect, deter or prevent potential criminal activities such as fraud, money laundering, etc.;
- Enhance quality of our services and products such as undertaking technical actuarial analysis based on personal data to determine optimal pricing, terms and conditions of our insurance products, undertaking customer survey by obtaining feedback to enhance our service delivery, etc.; or
- Undertake any other legitimate interest, as the case may be.

The KDPA allows us to use the personal data we collect as set out above on the basis that the processing is necessary for the performance of a contract with you, or when acting in our legitimate business interests. In doing this, we endeavor to adhere to the principle of purpose limitation and will only process your personal data for the sole purpose specified when the data is being collected from you. The use of your personal data in this nature and context is subject to your rights as provided for under the KDPA.

Overall, the lawful basis that we rely upon for processing your personal information is guided by the KDPA and associated regulations and may include one or several of the following:

a) Where we have your consent, which you are able to withdraw at any time by contacting the Company's Data Protection Officer (DPO);
b) Where we have a contractual obligation;
c) Where we have a legal obligation;
d) Where we have a vital or legitimate interest; or
e) Where we need it to perform a specified public duty.

When you provide your personal information to us under any of the above circumstances, you consent that it can be used for the specified purposes and that you or your entity is an authorized holder of such information.

Where you have provided us with personal data relating to other third parties, which you or your authorized agent have directly collected from them, you are expected to have obtained prior consent from the respective data subjects to process their personal data and share with us.

6. Sharing your personal data

In the normal course of business, we may share personal data provided by you with other third parties for various legitimate business interests or in compliance with applicable laws and regulations. In this regard, we may share such personal data with the following categories of third parties:

- Government authorities, law-enforcement agencies and relevant regulatory bodies (e.g. IRA) in compliance with legal and/or regulatory requirements;
- Business partners, associates, intermediaries and other players within the insurance and reinsurance supply chain. This could include our retrocessionaires, re-insurance brokers and agents, actuaries, assessors, loss adjusters, etc.;
- Relevant industry associations such as the Association of Kenya Reinsurers (AKR) for the purposes of industry analysis and advancement of the policy framework within the insurance industry;
- Competent information technology (IT) service providers who provide and support our technology and infrastructure needs around data management and security, including data back-up services;
- Our professional advisors and consultants such as the auditors, legal advisors, actuaries and financial advisors etc.; or
- Any other relevant third party legally permitted to process your personal data in furtherance of various legitimate interests.

We shall in all circumstances, where feasible and legally justifiable, inform and seek consent from you prior to sharing personal data with third parties.

7. International transfer of your personal data

Prior to transferring personal data outside Kenya, we shall ascertain that the transfer is based on the provided legal and regulatory standards and frameworks. Circumstances (and

corresponding legal basis) in which we may transfer your personal data outside Kenya are highlighted in the table below:

Circumstances	Legal basis
Where there is need to store (back-up) personal data in a cloud-based data server located in a country that has implemented data protection laws equivalent to the KDPA, such as the EU General Data Protection Regulation.	There being appropriate data protection safeguards with respect to the security and protection of personal data in respect to the jurisdiction to which the data is being transferred to.
Where the Data Commissioner has published a list of countries which have appropriate data protection safeguards and we decide to store the data in that jurisdiction in furtherance of our legitimate interest.	An adequacy decision having being made by the Office of the Data Commissioner.
Where we are obligated to meet our obligations under our reinsurance contracts and/or service contract with you.	Binding corporate rules (i.e. Necessity).
When following your express consent to transfer your personal data to another jurisdiction.	Consent of the data subject.

8. Securing and storing your personal data

Information security is extremely important to us. In this regard, we have put in place appropriate technical, physical, legal and organizational security measures to keep your Personal Information safe and secure. Such measures include, among others:

- Use of anti-virus protection systems, firewalls, and data encryption technologies;
- Ensuring that access to specified sensitive and personal data is restricted to relevant staff members as determined under various business processes using systems rights;
- Use of Data Loss Prevention engine which restricts system users access and transfer of unauthorized sensitive data to their personal folders, external data storage devices, or any device outside our network;
- Regular training to our staff on data protection requirements and IT and cyber security measures; and
- Undertaking annual independent IT systems audit and vulnerability assessment and penetration testing to assess the level of cyber-risk maturity.

Given that most of the personal information we hold is stored electronically, we have invested in appropriate electronic data management system in addition to implementing appropriate IT security measures and data back-up systems (physical and cloud-based) to ensure your personal information is safe and secure but also accessible.

Where we have engaged a third party (including our service providers) to collect or otherwise process personal information on our behalf, the third party will be selected with due care and required to use appropriate security measures to protect the confidentiality and security of personal information.

9. Retention of personal data

We retain personal information for as long as is necessary for the purposes for which we collect it, and in accordance to the KDPA and the Company's internal Data Retention and Disposal Policy. In addition, as a regulated financial services institution, certain laws and regulations apply to us which set minimum periods for retention of Personal Information.

Generally, the law requires us to retain your personal data for a minimum period of 7 years at which point the information shall be removed from our IT systems or physical storage space and either deleted, destroyed or archived.

10. Managing breach of personal data

We have in place robust measures to minimize and prevent data privacy and security incidents relating to personal data that we process. This includes appropriate reporting channels as guided by our Data Privacy and Protection framework and the KDPA.

We constantly monitor the threat environment and have prepared lines of communication both internally and externally with the Office of the Data Commissioner. Our framework and policies aim to mitigate and resolve such incidents in order to minimize harm to the Company and to you as the data subject.

Should a breach of personal data occur (whether in respect of you or someone else) then, we must keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of the data subject then, the Company must also notify the Data Commissioner's Office within 72 hours.

11. Your rights

Under the Kenyan Data Protection laws and regulations, you have the following rights in relation to your personal data:

i. *The right of access* - You have the right to ask us for copies of your personal information and obtain information on how the said personal data is used and processed.
ii. *The right to rectification* - You have the right to ask us to rectify personal information that you think is inaccurate. You also have the right to ask us to complete information that you think is incomplete.
iii. *The right to erasure* - You have the right to ask us to erase your personal information from our records in certain circumstances.
iv. *The right to restriction of processing* - You have the right to ask us to restrict the processing of your personal information in certain circumstances.
v. *The right to object to processing* - You have the right to object to the processing of your personal information in certain circumstances.
vi. *The right to data portability* - You have the right to ask that we transfer the personal information you gave us to another organization, or to you, in certain circumstances.

While your rights and fundamental freedoms are protected and safeguarded in line with provisions of the KDPA, these rights are not always absolute and may be subject to other applicable laws.

In exercising your rights as prescribed above, you are not required to pay any charges or fees. However, we reserve the right to apply a "nominal fee" in exceptional circumstances where the request is deemed excessive or onerous.

12. Use of Cookies

Cookies are small data files sent by a web server to a web browser, processor memory or hard drive (such as your computer or smartphone) and stored there. They are used for different purposes such as customizing a website for a specific user, analyzing the performance and design of a website, and improving the overall user experience not limited to storing the said user's preferences and login information. Cookies can be classified as follows:

- *Essential cookies (strictly necessary cookies):* They are explicitly used to facilitate the transmission of communications over a network; or to provide an online service on a website (e.g. in this case, a service you have requested in our website).
- *Non-Essential cookies (analytical cookies):* These cookies do not fall within the definition of essential cookies and are used to analyze your behavior on the website.
- *Session cookies:* These cookies are only active within the period your browser is open or a website is launched and expire as soon as the browser is closed or you leave a website.
- *Persistent cookies:* These cookies are stored on your device for a specific amount of time, after which they expire and are automatically deleted. They can however be manually deleted by the user before the set time.

We use Essential cookies, Non-Essential cookies and Session cookies to monitor our website performance and analyze the frequency of site visits. We analyze the type of traffic and geographical location not limited to; the type of end-user device, browser type and operating system.

The information we receive from the cookies is non-personal, aggregated and anonymous such as: the IP address of your computer, the date and time of your visit, which pages you browsed and whether the pages have been delivered successfully.

You may disable or set preferences on which cookies may apply to you through the cookie settings on your browser. However, please be aware that if you do turn off 'cookies' in your browser, you will not be able to fully experience our website.

13. Enforcing your rights, Complaints and Enquiries

Should you wish to enforce any of your rights or have any complaints, concerns or enquiries about our use or processing of your personal information, please contact our Data Protection Officer (DPO) using the contact details below or visit our offices. We will respond to your enquiries without undue delay and within the statutory timelines.

The Data Protection Officer
East Africa Reinsurance Company Limited
EARe House, 98 Riverside Drive
Post Office Box: 20196 – 00200, Nairobi
Email Address: dpo@eastafricare.com
Telephone No. +254 20 4084301

You may also launch a complaint if you are unhappy with how we have used your personal data directly through the Office of the Data Commissioner at the address below:

The Office of the Data Commissioner
Britam Tower, Hospital Road, Upper-hill, Nairobi, Kenya
Post Office Box: 30920-00100; G.P.O Nairobi
Email Address: info@odpc.go.ke
Telephone No. +254 796954269 / +254 778048164

14. Changes to this privacy notice

The Company keeps this privacy notice under regular review to make sure it is up to date, accurate and in line with changes in regulatory landscape on data protection. The latest version will govern our use of your information and by continuing your relationship with us or accessing our website after any changes have become effective, you agree to accept the revised privacy notice.

Please visit this privacy notice on our website www.eastafricare.com to ensure that you have read the latest version.