

EXIM BANK (UGANDA) LIMITED PRIVACY STATEMENT

VERSION 3 [Revised June 2025]

Exim Bank (Uganda) Limited respects the right to privacy of our clients, the people with whom we engage during our dealings with our clients and other relevant persons. These include, but are not limited to, employees, officers, directors, beneficial owners, and other personnel of our clients, service providers and other business counterparties (herein referred to as “data subject”). Any personal information collected is treated with the highest standards of security and confidentiality in accordance with the Data Protection and Privacy Act Cap 97-Laws of Uganda.

A. . Consent to Access personal data

We collect personal data directly from the data subject through various sources, including, but not limited to National Identity Cards, Passports, Refugee/Alien Identity Cards, Driving License, Company/Business Legal documents, Property ownership documents and others.

We may also collect and verify the authenticity and accuracy of personal information about the client or vendor or employee from public sources or legally recognized secondary sources such as government agencies, including, but not limited to, National Identification Register (NIR), Office of the Prime Minister (OPM), Ministry of Internal Affairs (Directorate of Citizenship & Immigration Control), Uganda Registration Services Bureau (URSB), institutions of learning and other personal data controlling bodies/institutions.

By accepting to engage in any kind of business relationship or contractual obligation or to consume Bank services, the customer or legal guardian or representative consents that the Bank shall have the right to apply and have access to his/her personal information contained in the National Information Register or other data collecting or processing or controlling authority or institution, as described by whatever name or nature.

B. Nature of personal data collected.

The Bank collects all personal data that is necessary to pursue legitimate business and other interests. Data collected includes, but is not limited to, names, gender, resident status, sensor data, contact details, transaction profiles, political exposure status, biometric data, financial history, property ownership documents (certificate of title,

B

atul

motor vehicle registration card, utility bills) and others, medical history & generic data (Bancassurance services).

C. Requirement to collect personal data.

The provision of personal data is mandatory.

D. Failure to provide personal data.

If a data subject does not provide information as requested, the Bank may not be able to provide or to continue providing relevant products, services or otherwise do business, with the subject client, service provider or any business counterparty.

E. Purpose of personal data collected.

Personal data collected is used to pursue the Bank's legitimate business and other interests as listed below:

1. Provision of financial services and products to our clients for example opening & maintenance of account numbers, advance of credit facilities, insurance services and others.
2. Communication with our clients about the Bank's products & services. The Bank may send promotional materials or details by SMS, E-Mail, or post in order to update clients, service providers and business counterparties on any promotions, news, competitions or developments. Data subjects are advised to cautiously consider information disseminated on the open media Bank channels capable of being utilized by any person for example Social media platforms like facebook, X, Tiktok etc.
3. To manage, administer & improve our business through clients and service provider engagements and relationship management.
4. For marketing, analysis & business development to ensure satisfactory service delivery.
5. To investigate and respond to complaints or incidents relating to the Bank or our business and to train staff to deal with complaints and maintain service quality.
6. To comply with laws and regulations.

F. Processing of personal data.

In order to pursue the Bank's legitimate interests and in cooperation with our regulators and other statutory authorities and for purposes of complying with local, foreign or international law, preventing and detecting financial and other crimes and regulatory breaches, and protecting our businesses and the integrity of the financial system, the Bank processes personal data collected for the below reasons.

1. To monitor and analyze the use of our products and services for system administration, operation, testing & support purposes.

ba

full

2. To monitor and analyze the use of our products and services for risk assessment and control purposes, including but not limited to, detection, prevention, and investigation of fraud.
3. To manage our information technology and to ensure the security of our systems.
4. To establish, exercise and/or defend legal claims or rights and to protect, exercise, and enforce our rights, property, or safety, or to assist our clients, service providers or business counterparties to do the same.
5. To cooperate with, respond to requests from, and to report transactions and/or other activity to government, tax or regulatory bodies, financial markets, brokers, Courts or other intermediaries or counterparties, or authorized third parties.
6. To conduct compliance activities such as audit & reporting, assessing & managing risk, maintenance of accounting & tax records, fraud, Anti-Money Laundering (AML) prevention and measures relating to sanctions, Anti- Terrorism laws and fighting financial crime.
7. To conduct due diligence activities such as Know Your Customer (KYC) screening (this includes identity verification & checks on address & contact details); Politically Exposed Persons (PEPs) which involves screening client records against internal and external databases to establish connections to PEPs; and sanctions screening (which involves the screening of clients, service providers and business counterparties, and their representatives against published sanctions lists.
8. To record and monitor telephone conversations to maintain service quality and security, and for fraud monitoring, complaints handling, disputes, potential and/or actual criminal activity. To the extent permitted by law, these recordings are the Bank's sole property.

G. Disclosure of personal data.

The Bank discloses personal information for the reasons set out in section F as follows.

1. To service providers, and other business counterparties in connection with the products and services that we provide.
2. To the Bank group entities for purposes of managing Exim Bank (Uganda) Limited's client, service provider and other business counterparty relationships.
3. To counterparty banks, payment infrastructure providers and other persons from whom we receive, or to whom we make payments on our clients' or service providers' behalf.
4. To export credit agencies, multilateral agencies, development finance institutions, other financial institutions, government authorities and their agents, insurers, due diligence service providers and credit assessors, in each case in connection with the products and services we provide, including financings.

b

allu

5. To service providers that provide application processing, fraud monitoring, call center and/or other customer services, hosting services and other technology and business process outsourcing services.
6. To professional service providers, such as legal advisors, accountants, auditors, insurers, tax advisors and others alike.
7. To competent regulatory, prosecuting, tax, courts/tribunals in any jurisdiction, government, law enforcement authorities and other persons involved in, or contemplating, legal proceedings.
8. To prospective buyers as part of a sale, merger, or other disposal of any of our business or assets.
9. To other persons where disclosure is required by law or to enable products and services to be provided to the data subject.

H. Third Parties

It is mandatory for the Bank's service providers and other business counterparties to subscribe and adhere to our privacy policy.

I. Cross Boarder Data Sharing.

The Bank may share the data subject's personal data with foreign service providers to enable service delivery. Data may only be shared with foreign service providers or business counterparties or in accordance with section F, where the legal framework regarding data privacy and protection is similar to the safeguards in Uganda, and upon execution of an agreement that covers protection and confidentiality of the shared data.

J. Data retention.

The Bank retains personal data collected & processed for as long as is necessary for the purposes of our relationship with you or in connection with performing an agreement with the data subject, service provider or business counterparties or complying with a legal or regulatory obligation.

K. Personal data update

To ensure data accuracy & effective service delivery, data subject, customers and service providers should keep the Bank updated with any change in personal data details, at their own initiative or whenever called upon by the Bank.

L. Technical Security.

The Bank's security systems are designed to prevent loss, unauthorized access, damage and/or access to client personal information by unauthorized persons.

M. Rights to Personal Information.

The data subject may;

1. Request the Bank for a copy of their personal data. This right does not extend to data processed by the Bank. b
2. Request the Bank to correct their personal data.

-mm

5. To service providers that provide application processing, fraud monitoring, call center and/or other customer services, hosting services and other technology and business process outsourcing services.
6. To professional service providers, such as legal advisors, accountants, auditors, insurers, tax advisors and others alike.
7. To competent regulatory, prosecuting, tax, courts/tribunals in any jurisdiction, government, law enforcement authorities and other persons involved in, or contemplating, legal proceedings.
8. To prospective buyers as part of a sale, merger, or other disposal of any of our business or assets.
9. To other persons where disclosure is required by law or to enable products and services to be provided to the data subject.

H. Third Parties

It is mandatory for the Bank's service providers and other business counterparties to subscribe and adhere to our privacy policy.

I. Cross Border Data Sharing.

The Bank may share the data subject's personal data with foreign service providers to enable service delivery. Data may only be shared with foreign service providers or business counterparties or in accordance with section F, where the legal framework regarding data privacy and protection is similar to the safeguards in Uganda, and upon execution of an agreement that covers protection and confidentiality of the shared data.

J. Data retention.

The Bank retains personal data collected & processed for as long as is necessary for the purposes of our relationship with you or in connection with performing an agreement with Public the data subject, service provider or business counterparties or complying with a legal or regulatory obligation.

K. Personal data update

To ensure data accuracy & effective service delivery, data subject, customers and service providers should keep the Bank updated with any change in personal data details, at their own initiative or whenever called upon by the Bank.

L. Technical Security.

The Bank's security systems are designed to prevent loss, unauthorized access, damage and/or access to client personal information by unauthorized persons.

M. Rights to Personal Information.

The data subject may;

1. Request the Bank for a copy of their personal data. This right does not extend to data processed by the Bank.
2. Request the Bank to correct their personal data.

b

—

3. Request for erasing of their personal data, subject to data retention obligation as by law established.
4. Restrict the processing of their personal data.
5. An aggrieved data subject may also lodge a complaint with the Personal Data Protection Office of Uganda by visiting www.pdpo.go.ug.

N. Amendment of this privacy statement.

The Bank reserves the right to amend this privacy statement at any time and a new version will always be posted to the Bank's website.

The Bank advises clients to acquaint with the Uganda Data Privacy and Protection Act which can be found at [Data-Protection-and-Privacy-Act-2019.pdf \(ict.go.ug\)](#)

CLIENTS ARE ALSO ADVISED TO FOLLOW THE SAFETY TIPS PUBLISHED ON OUR WEBSITE: eximbank-ug.com

For Inquiries, contact the Data Protection Officer- Newton Ferdinand Oturuke on; newton.oturuke@eximbank-ug.com +256 312320400 (8:30 am – 5:30 pm weekdays)

Terms & Conditions Apply.

Exim Bank (Uganda) Limited is Regulated by Bank of Uganda. Customer Deposits are Protected by the Deposit Protection Fund of Uganda up to Ugx 10 million, Terms & Conditions Apply

 