



**Empower Your
Everyday Business**

Privacy Policy

[Home](#) > [Privacy Policy](#)

1. PURPOSE AND SCOPE OF THIS POLICY

At Pearl Bank Uganda Limited ("Pearl Bank", "the Bank", "we", "our" or "us"), protecting your personal information is fundamental to the trust you place in us. This Privacy Notice explains how we collect, use, store, disclose, transfer, and protect personal information relating to individuals who interact with our Bank services or Platforms that is its branches, digital channels, products, services, websites, applications and other channels. It applies to customers, prospective customers, authorized representatives, beneficiaries, guarantors, merchants, agents, service providers and other individuals whose personal data the Bank processes. We are committed to handling your personal information in a lawful, transparent, and secure manner, in accordance with the Data Protection and Privacy Act, the Data Protection and Privacy Regulations, and other applicable laws and regulations of Uganda. By opening an account, registering for, accessing, or using our Platforms, you acknowledge that you have read and understood this Privacy Notice.

2. WHO WE ARE

Pearl Bank is a financial institution licensed and regulated by the Bank of Uganda. For purposes of applicable data protection laws, Pearl Bank acts as a Data Controller where it determines the purposes and means of processing personal data and may act as a data processor where it processes personal data on behalf of another controller. The Bank is responsible for processing personal data fairly, lawfully and transparently, collecting adequate and relevant data, maintaining accuracy, applying appropriate security safeguards and retaining data in accordance with applicable law.

3. INFORMATION WE COLLECT

To provide secure and efficient banking services, we collect information about you which may include the following:

3.1 Identification and KYC Information

Full name; date of birth; nationality; National Identification Number; passport or other identity document details; photograph; signature; tax identification details; customer/account identifiers; and information required for customer due diligence.

3.2 Contact and Address Information

Telephone numbers; email addresses; residential, postal and physical addresses; employment or business contact details and other contact information.

3.3 Financial and Banking Information

Account details; balances; transaction history; payment and transfer instructions; source of funds or wealth where required; income and expenditure information; loan and credit information; card and payment information; beneficiary details and other information necessary to provide banking services.

3.4 Representatives and Related Persons

Information about directors, shareholders, beneficial owners, authorized signatories, administrators, guarantors, beneficiaries, next of kin and other persons connected to a customer or transaction where required for banking, legal, regulatory or security purposes.

3.5 Digital, Device and Technical Information

Device identifiers; IP addresses; browser and operating system information; login dates and times; session activity; system and security logs; authentication information and other technical information generated through use of digital channels.

3.6 Location Information

Approximate location information where enabled and legally permissible, including where necessary for security, fraud prevention or functionality.

3.7 Communications and Service Interaction Information

Records of correspondence, enquiries, complaints, service requests, call recordings where applicable and information provided during interactions with the Bank.

3.8 Business and Merchant Information

For business, merchant and agency relationships, business registration details, business contacts, ownership and management information, authorized representative details, settlement account information and other information required for KYB, AML/CTF and service delivery.

3.9 Information Obtained from Other Sources

Where permitted or required by law, information may be obtained from credit reference bureaus, government authorities, identity verification providers, payment networks, correspondent banks, sanctions/watchlist providers, fraud prevention providers, regulators and other lawful sources.

4. HOW WE COLLECT PERSONAL DATA

We generally collect personal data directly from you through account opening and service forms, branch interactions, digital and mobile banking channels, websites, applications, customer service interactions and other communications. Where permitted by law, we may also collect information from authorized representatives, public records, regulators, credit reference bureaus, government or identity verification sources and other third parties.

Before collecting personal data, the Bank will provide information appropriate to the circumstances, including the nature and categories of data, purpose of collection, whether provision is mandatory or discretionary, consequences of failure to provide it, relevant recipients and applicable data subject rights.

5. HOW WE USE YOUR INFORMATION

We use your personal information to provide and manage banking services, process transactions, verify customer identities, and ensure secure access to our Internet Banking Platform. We also process your information to comply with legal and regulatory requirements, including KYC and anti-money laundering obligations, detect and prevent fraud, protect customer accounts and Bank systems, improve our products and services.

Where permitted by law and subject to your preferences, we may send information about our products, services, promotions, and events. You may opt out of receiving marketing communications at any time.

6. **LAWFUL BASIS FOR PROCESSING**

We process personal information only where you have provided consent and where it is necessary to provide the banking services as requested by you and perform or enter into a contract. We also process your personal information where it is required by law or regulation and where it is necessary to execute a legitimate business interest, provided that such interests do not override your rights and freedoms. Where processing is based on consent, withdrawal will not affect processing already carried out lawfully before withdrawal and may not stop processing that is otherwise authorized or required by law or necessary for another lawful purpose.

7. **OUR COMMITMENT TO DATA PROTECTION**

We process personal data in line with applicable data protection principles. The Bank collects and uses only data that is adequate, relevant, and necessary for the intended purpose. We take reasonable steps to keep personal data accurate and up to date and to correct any inaccurate or incomplete information. Personal data will not be used for purposes that are incompatible with the original purpose unless permitted by law or supported by another lawful basis.

8. **SHARING AND DISCLOSURE OF INFORMATION**

We treat customer information as confidential. However, we may share information where necessary with technology service providers, payment processors, correspondent banks, regulatory authorities, auditors, legal advisors and other designated partners. We only share information where there is a lawful basis to do so and appropriate confidentiality safeguards are in place. We do not sell personal information to third parties.

9. **CROSS-BORDER DATA TRANSFERS**

We and some of our service providers, payment networks, and technology partners may process information outside Uganda. Where personal information is transferred outside Uganda, we ensure that appropriate legal safeguards and security measures are in place, the recipient provides an adequate level of protection, and the transfer is permitted under applicable laws.

10. **DATA RETENTION**

We retain personal information only for as long as it is necessary to provide the services you seek or request, meet legal and regulatory obligations, resolve disputes, enforce contractual rights and maintain business and audit records. Retention periods may be determined by banking regulations, anti-money laundering requirements, taxation laws, and other applicable legal obligations. When information is no longer required, it is securely deleted, anonymized, or destroyed.

11. **HOW WE KEEP YOUR INFORMATION SECURE**

Protecting customer information is a key priority for us. We maintain reasonable physical, technical, and administrative safeguards, including but not limited to Encryption of data in transit and at rest, multi-factor authentication, Secure access controls, User activity monitoring, Network security controls, data loss prevention, third party security controls, Security awareness training for employees and independent security testing and assessments. You also play an important role in protecting Your information and should safeguard usernames, passwords, tokens, and other authentication credentials.

12. **DATA BREACH MANAGEMENT**

No transmission or storage method is completely secure. The Bank will handle suspected data security incidents in accordance with applicable law and its incident response procedures. If an incident results in unauthorized access to personal information, we will promptly investigate and take appropriate corrective action. Where required by law, we will notify affected individuals and relevant regulatory authorities within the prescribed timelines.

13. **YOUR RIGHTS**

Subject to applicable law, you have the right to:

- Access your personal information;
- Request correction of inaccurate or incomplete information;
- Request deletion of information in certain circumstances;
- Object to certain processing activities;
- Restrict the processing of personal information in specific situations;
- Withdraw consent where processing is based on consent;
- Request details regarding how your information is processed;
- Request review of certain automated decisions.

To protect your information, we may require proof of identity before processing a request and maybe subject to lawful exemptions, limitations and the rights of other persons.

14. **AUTOMATED DECISION-MAKING**

To help protect customers and comply with regulatory requirements, we may use automated tools for fraud detection, transaction monitoring, risk assessment and cybersecurity monitoring. Where an automated decision produces a significant effect on you, you will be informed within reasonable time and accorded a chance to review the decision.

Where permitted by law and subject to applicable preferences, the Bank may send information about products, services, promotions and events. You may request that the Bank stop processing your personal data for direct marketing. The Bank will respond in accordance with applicable law.

15. **COOKIES**

Our Platform uses cookies and similar technologies to maintain secure login sessions, improve Platform functionality, remember user preferences, Measure system performance and enhance the customer experience. Certain cookies are essential for the operation and security of the Platform and cannot be disabled. You can follow the instructions provided by your browser to modify your cookie settings, however, please note that if you set your browser to disable cookies, certain services may not function properly.

16. **CHANGES TO OUR PRIVACY NOTICE**

We may update this Privacy Notice from time to time to reflect changes in our services, technology, legal obligations, or business practices. Where significant changes are made, we will notify customers through appropriate channels, including our website, internet banking platform, email, or other communication methods. The latest version of this Privacy Notice will always be available through our official channels.

17. **CONTACT US**

You also have the right to lodge a complaint with the Personal Data Protection Office (PDPO) if you believe your personal information has been processed in a manner that is inconsistent with applicable data protection laws.

If you have questions about this Privacy Notice, wish to exercise your privacy rights, or would like further information about how we process your personal information,

Please contact our:

Data Protection Officer
Email: dpo@pearlbank.com | **Telephone:** +256 (0)417-157 780

Branch, ATM, and Agent Locator

Region ▾

Branches ▾

Locate



WHO WE ARE
About Pearl Bank Uganda
Board Members
Awards and Recognitions
Careers
FAQs
Contact Us
Privacy Policy

NEWS ROOM
Products and Services
Press Releases
Gallery
Stories

Head Office:
Pearl Bank Uganda Limited
Plot 15-17 Roscoe Road, Kololo

Tel:
0800 217200 (TollFree),
0417 157 200

Whatsapp:
+256 707 993 930

Email:
customerservice@pearlbank.co.ug

Pearl Bank Uganda (PBU) is a public company limited by shares and formed under the Public Enterprises Reform and Divestiture Statute of 1983 and the Uganda Communications Act, 1997.

