PRIVACY NOTICE

Ensuring the Privacy, Security, and Confidentiality of Your Personal Data w.e.f 01st June 2026 (*Version 1.1*)

1. Introduction

At Pan Asia Banking Corporation PLC, we recognize the importance of protecting your personal data. This Privacy Notice explains our data protection practices and outlines:

- ❖ What Personal Data do we collect.
- ❖ How we process, use, and store your information.
- ❖ Who we may share your data with.
- ❖ How we protect your personal data and the security measures we implement.
- ❖ Your rights under the Personal Data Protection Act, No. 9 of 2022 (PDPA).
- ❖ How you can contact us for inquiries regarding your data.

Where applicable, additional privacy disclosures may be provided separately for specific products, services, business functions, or interactions to ensure transparency in how we handle your information.

In this Privacy Notice, "we," "us," or "our" refers to Pan Asia Banking Corporation PLC, which acts as the data controller for your personal data.

> What is a Data Controller?
>
> A data controller determines the purposes and means of processing your personal data and is responsible for ensuring compliance with the Personal Data Protection Act, No. 9 of 2022 (PDPA).

2. Scope of this Privacy Notice

Wherever we say 'you' or 'your', this refers to:

- You as an individual customer or account holder.
- Anyone acting on your behalf, such as trustees, executors, or individuals with power of attorney.

- Other related persons, such as authorized signatories, partners, or legal representatives.

This Privacy Notice applies to:

1. Banking Customers – Individuals who hold accounts, use our products or services, or interact with our banking operations.
2. Visitors and Other Non-Clients – Individuals who visit our premises, website, or interact with us without being direct customers.
3. Job Applicants – Individuals who apply for employment opportunities.
4. Vendors and Service Providers – Third parties who provide services to or collaborate with the Bank.

This Privacy Notice does not apply to third-party websites, applications, or services that we do not operate or control.

If you have any questions or concerns regarding your personal data, please refer to the "Contact Us" section for the relevant contact details.

3. Our Privacy Principals

At PABC Corporation PLC, trust is the foundation of our relationship with our customers. To uphold this trust and ensure the confidentiality of your personal data, we adhere to the following principles:

- We collect only the necessary personal data required to understand your financial needs and conduct our banking operations.
- We use your personal data responsibly to provide you with enhanced banking services and tailored financial products.
- We do not disclose your personal data to third parties without your consent unless required by law or regulatory obligations.
- We ensure strict security measures to protect your personal data from unauthorized access, loss, or misuse.
- We strive to maintain accurate and up-to-date records of your personal data.
- All employees and authorized third parties handling your personal data are bound by strict confidentiality obligations.

By adhering to these principles, we reaffirm our commitment to protecting your personal data and maintaining the trust you place in us.

4. What personal information do we collect?

PABC collects and processes your personal data to provide our products and services, manage our relationship with you, and operate our business efficiently. This applies whether you hold an account with us or are connected to another individual or entity banking with us, such as a guarantor, employee, shareholder, director, officer, or authorized representative.

IDENTIFICATION DATA	CONSENT & PREFERENCES MANAGEMENT	CONTACT DETAILS

• Full Name, Gender, Date of Birth
• National Identity Card (NIC), Passport, Driving License, Tax Identification Number (TIN)
• Nationality & Residency Status (including tax residency, if applicable)
• Financial & Banking Details (Account Numbers, Loan Records, Credit History, Transaction Details)
• Spouse, Dependents, and Guardian Information
  ▪ Names & Relationship to the Account Holder (e.g., Spouse, Child, Legal Guardian)
  ▪ Identification Details (NIC, Passport, Birth Certificate, or other official ID where applicable)
  ▪ Guardian’s Legal Authority (e.g., Power
	• Marketing opt-ins/opt-outs
	• Cookie preferences for website users
	• Data Subject Requests under PDPA
		• Address, Work Address
		• Personal & Work Email, Personal & Work Telephone Numbers

of Attorney, Custodianship, or Court Order) • Health Information (Medical records)		
ONLINE & DIGITAL BANKING INTERACTIONS	YOUR INCOME AND BENEFITS	EMPLOYMENT, RECRUITMENT DATA & HR DATA
• IP Address • Login Attempts, Failed Logins, or Behavioral Analytics • Login Credentials	• Salary • Bonus • Commission entitlements, raise amounts and percentages • Pension plans	• Employee ID, Job Title • EPF/ETF Contributions, Salary, Bonus, Commission, Pension Plans • Performance Evaluations & Disciplinary Records • Resignation, Termination, or Exit Interview Data • CVs/Resumes, cover letters, and job application forms
BUILDING ACCESS MONITORING INFORMATION	CALL CENTER, COMMUNICATIONS AND SOCIAL MEDIA	THIRD-PARTY & EXTERNAL DATA SOURCES
• CCTV images • Details of visits to our premises. • Biometrics	• Emails and letters • Call Logs, Customer Service Interactions, Chatbot Conversations	• Credit Score Data (from CRIB or other sources) • Sanctions Screening & Watchlist Data

	• Voice Recordings • Customer Complaints • Dispute Resolution Records	

*The personal data types mentioned above are for example purposes only, and the list is not exhaustive.

5. Methods of Personal Data Collection

At PABC, we are committed to collecting and handling your personal data responsibly. This section explains how we collect personal information in compliance with the Personal Data Protection Act.

Use of Cookies & Online Tracking

When you visit our website, mobile applications, or online banking platforms, we may use cookies and similar tracking technologies to:

- Enhance user experience and navigation.
- Analyse website traffic and service usage.
- Improve security and fraud detection measures.

You can manage or disable cookies through your browser settings. However, disabling certain cookies may limit access to online banking features. For more details, please refer to our Cookie Notice.

How We Collect Your Personal Data

We collect personal data through multiple channels, including:

Direct Collection

- When you apply for banking products or services (e.g., account opening, loan applications, card services).
- When you use our online banking, mobile banking, or visit our branches.
- When you contact us via phone, email, or in person for inquiries or transactions.

- When you submit CVs, cover letters, or job applications via our career's portal, email, or in person.

Third-party sources *(Where legally permitted and necessary for banking operations)*

- Regulatory authorities and law enforcement agencies (e.g., for compliance, fraud prevention, and financial crime monitoring).
- Credit bureaus and financial institutions (e.g., for credit assessments, loan processing, and risk evaluations).
- Payment service providers and transaction processors (e.g., VISA, Mastercard, SWIFT, etc.).
- Recruitment agencies or headhunters to identify potential candidates

Publicly Available Sources

- Government databases, tax registries, and regulatory authorities (e.g., Central Bank, Financial Intelligence Unit, Department of Registrar of Companies).
- Court judgments, insolvency records, and public financial sanctions lists (for due diligence and risk assessments).
- Company registration databases for corporate banking verification.
- For recruitment and talent acquisition, we may collect personal data from Professional networking platforms (e.g., LinkedIn).

Social Media & Business Directories – Only Where Customer Provides Data

- We do not actively collect personal data from social media or networking sites.
- If a customer engages with us via social media (e.g., Twitter, Facebook customer support channels), we may collect only the information voluntarily provided by the customer.

6. Legal Basis for Processing Your Personal Data

We process personal data based on the following lawful grounds under the Personal Data Protection Act, No. 9 of 2022, and other applicable regulations:

- Contract

  When processing is necessary to fulfil contractual obligations.

- Legal Obligation

When required to comply with legal, regulatory, or industry obligations.

- Legitimate Interest

  When processing is necessary for the Bank's legitimate business interests, provided it does not override your rights and freedoms.

- Consent

  When legally required, such as for marketing, certain background checks, or processing sensitive personal data.

For sensitive personal information, we will only process it if:

- You have given explicit consent.
- The information has been made manifestly public.

7. How Do We Use Your Personal Data? (Purposes of Processing)

We process personal data for the following lawful and necessary purposes:

General Business Operations (Applies to All Data Subjects)

- Performing administrative, compliance, and operational tasks related to account management, regulatory reporting, and financial oversight.
- Conducting risk assessments and internal audits to ensure regulatory compliance and operational integrity.
- Recording communications (e.g., phone calls, emails, chat interactions) for quality control, compliance, and dispute resolution.
- Maintaining the security and functionality of digital banking platforms, mobile apps, and online services.
- Facilitating internal training, process improvement, and staff development using anonymized customer interactions.
- Using data analytics and machine learning to personalize banking services, refine marketing strategies, and enhance customer engagement.
- Testing and evaluating new banking systems, digital platforms, and security controls to enhance performance and security.

- Transferring client records to an acquiring entity in the event of a corporate restructuring, legal merger, or ownership change.
- Sending promotional offers, newsletters, and banking product updates based on customer preferences and prior interactions.
- Engaging in loyalty programs, referral incentives, and reward schemes where applicable.
- Hosting promotional events, webinars, and sponsorship activities.

For Banking Customers

- Conducting Know-Your-Customer (KYC) and due diligence checks to prevent fraud and ensure compliance with financial regulations.
- Assessing and managing credit risk, setting credit limits, and conducting financial assessments for loan and credit applications.
- Processing transactions, including fund transfers, bill payments, deposits, and withdrawals.
- Handling customer service inquiries, complaints, and dispute resolution.
- Detecting, investigating, and preventing financial crimes, including Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and fraud detection.
- Conducting behavioural analysis for security and fraud prevention, including monitoring suspicious transactions, location-based authentication, and login patterns.
- Ensuring business continuity through system backups, cybersecurity testing, and data recovery measures.

For Vendors & Service Providers

- Conducting vendor due diligence, risk assessments, and contract compliance monitoring.
- Processing payments, maintaining vendor accounts, and monitoring service performance.
- Ensuring compliance with anti-bribery policies, and tax regulations.
- Recording vendor communications for auditing, contractual performance tracking, and dispute resolution.

For Job Applicants

- Assessing job applications, conducting interviews, and verifying qualifications for recruitment purposes.
- Conducting pre-employment background checks, including identity verification, criminal record checks, and employment history validation.
- Maintaining recruitment records for workforce planning and audit purposes.
- Retaining CVs and applicant information for potential future job opportunities, where applicable and with the applicant's consent.
- Analysing recruitment data to improve the hiring process, optimize screening methods, and enhance workforce diversity strategies.

8. When Do We Conduct Direct Marketing?

We may use your contact details to send you marketing communications through channels such as post, email, telephone, SMS, secure messages, mobile apps, or social media platforms. These communications will be sent only with your consent.

If you have agreed to receive marketing communications, we may send you information about:

- News, promotions, and offers related to our banking, financial, and investment products and services.
- Exclusive banking privileges, rewards, and loyalty programs.
- Market research, customer experience surveys, and service feedback requests to improve our offerings.
- Invitations to seminars, webinars, financial literacy sessions, or banking-related events.

How We Personalize Our Marketing Efforts

To provide you with relevant and tailored marketing, we may use aggregated insights and demographic analytics based on your interactions, transaction patterns, and preferences. This allows us to recommend financial products and services that match your interests.

Your Right to Opt-Out

Marketing communications from the Bank are sent only with your **explicit consent**. You have the right to withdraw consent or opt out of receiving such communications at any time you receive the message and respond to the given phone number to opt out.

9. Data Sharing & Third Parties

We may share your personal data in accordance with legal, regulatory, and contractual requirements while ensuring that it remains confidential and protected. The categories of third parties we share your data with depend on your relationship with us and the nature of the services we provide.

Who May We Share Your Personal Data With?

We may share your personal data with:

Individuals & Entities Authorized by You *(If applicable to your banking relationship)*

- Joint account holders, co-signers, and authorized representatives.
- Legal guardians, beneficiaries, trustees, guarantors, or attorneys under a Power of Attorney.

Third Parties That Verify Your Information

- Credit bureaus, credit reference agencies, and debt collection agencies (for loan approvals, credit risk assessments, or financial recoveries).

Professional Service Providers & Advisors

- Auditors, legal counsel, and compliance advisors assisting with risk management, financial reporting, and regulatory compliance.
- Insurers and insurance brokers (where applicable to banking or loan-related insurance policies).

Technology & Operational Service Providers

- Cloud computing and IT security service providers that support digital banking, transaction processing, and cybersecurity measures.
- Third-party call centres and customer support providers assisting in service operations.

Financial Institutions & Payment Service Providers

- Payment processors, credit card networks, mobile wallet providers, and digital payment service operators (such as VISA, Mastercard, and other relevant payment service providers).

Government Authorities, Regulators & Law Enforcement Agencies

We may share your personal data as required by law or regulatory mandates, including with:

- Regulatory bodies, central banks, and financial authorities in jurisdictions where we operate.
- Government agencies, law enforcement, or judicial bodies in response to legal orders, tax obligations, or fraud investigations.

10. Where Do We Transfer Personal Data?

Your personal data may be processed, stored, shared, transferred, or disclosed by us within PABC or with authorized third parties both within and outside Sri Lanka for the purposes outlined in this Privacy Notice.

We transfer data to:

- Facilitate banking transactions and provide financial services efficiently and securely.
- Enhance and support our business operations, risk management, and compliance efforts.
- Ensure compliance with legal, regulatory, and industry obligations in different jurisdictions.

Cross-Border Data Transfers

In certain cases, we may transfer your personal data to jurisdictions outside Sri Lanka, which may not have data protection laws equivalent to Sri Lanka's Personal Data Protection Act.

To ensure your personal data remains protected, we implement appropriate safeguards, such as:

- Standard Contractual Clauses (SCCs) – Agreements that ensure third parties comply with data protection standards.
- Transfer Impact Assessments (TIAs) – We conduct risk assessments before transferring data across borders to evaluate the legal, regulatory, and security implications in the recipient country and ensure compliance with applicable data protection laws.

11. How Long Do We Keep Your Personal Data?

We retain your personal data for as long as necessary to fulfil the purposes outlined in this Privacy Notice, including business, operational, regulatory, and legal obligations. The retention period depends on the type of data, the nature of our relationship with you, and applicable legal requirements.

Retention & Deletion Practices

Active Engagement: While you are actively engaging with us (e.g., as a customer, vendor, or employee), we retain your personal data to provide services, maintain records, and meet compliance requirements.

Post-Engagement Retention: After your relationship with us ends, we may retain your personal data for:

- Regulatory & Legal Compliance: To meet statutory retention periods, comply with financial regulations, tax laws, and anti-money laundering (AML) obligations.
- Contractual & Dispute Resolution: To resolve disputes, enforce agreements, and handle claims or legal proceedings.
- Job Applicants: If you are not selected, your CV and related application data may be retained for 06 months for the purpose of considering you for future opportunities, unless you request your right to erasure as per the procedure mentioned below. If you are hired, your recruitment data will form part of your employee record and be retained in line with the Employee Privacy Notice.

Final Data Disposal: When your personal data is no longer required, we will:

- Delete or securely destroy it (if retention is no longer required).
- Anonymize it (where applicable) so that it can no longer identify you.
- Restrict further use in cases where retention is necessary, but processing is limited (e.g., archival or compliance records).

If you require further details about specific retention periods, you may request additional information by referring to the "**Contact Us**" section below.

12. Other Terms and Conditions

In addition to this Privacy Notice, the collection, use, and disclosure of your personal data may also be governed by specific terms and conditions outlined in our banking agreements, product terms, and service contracts.

These additional terms provide further details on how we handle personal data in the context of specific products, services, or transactions and must be read in conjunction with this Privacy Notice.

How Do We Protect Your Personal Data?

We take the privacy and security of your personal data seriously and have implemented a range of technical, physical, and organizational measures to ensure its confidentiality, integrity, and availability.

Our Security Measures Include:

1. ISO 27001 Certification – As an ISO 27001-certified bank, we adhere to internationally recognized information security standards, ensuring robust risk management, data protection, and cybersecurity controls.
2. Strong Access Controls – We enforce strict access management policies, ensuring that only authorized personnel can access personal data based on the principle of least privilege.
3. Encryption & Secure Data Transmission – We use encryption technologies to protect personal data both in transit and at rest, ensuring its security from unauthorized access or interception.
4. Incident Management & Breach Response – We have comprehensive incident detection, management, and reporting procedures in place to swiftly respond to data breaches or security threats in accordance with legal and regulatory requirements.
5. Third-Party Security Standards – Any third parties or service providers that process personal data on our behalf are required to comply with strict confidentiality, data protection, and security measures, including contractual agreements and ongoing security assessments.
6. Employee Training & Awareness – We regularly train our employees on data privacy best practices, regulatory compliance, and information security policies to prevent unauthorized access, misuse, or data breaches.

We continuously review, update, and strengthen our security measures to align with evolving cybersecurity threats and regulatory expectations

13. What Are Your Personal Data Protection Rights?

We respect your personal data rights under the Personal Data Protection Act, No. 9 of 2022 of Sri Lanka, and ensure that you can exercise them in accordance with applicable laws.

Under the Sri Lankan PDPA, you have the following rights regarding how we use and process your personal data:

1. Right to Access: You can request confirmation from us on whether your personal data is being processed and obtain a copy of such data, along with information on how it has been used.
2. Right to Rectification: If your personal data is inaccurate or incomplete, you have the right to request its correction or completion.
3. Right to Erasure: You may request the deletion of your personal data under certain circumstances, such as when the data is no longer necessary for the purposes it was collected or if you withdraw your consent upon which the processing is based.
4. Right to Withdraw Consent: If the processing of your personal data is based on your consent, you have the right to withdraw that consent at any time.
5. Right to Object to Processing: You can request us to refrain from further processing of your personal data under specific conditions, particularly if the processing adversely affects your rights and freedoms.
6. Right to Review Automated Decisions: If a decision significantly affecting you is made solely based on automated processing, you have the right to request a review of that decision.

14. How to Exercise Your Data Protection Rights

For Existing Customers (Active Account Holders)

- You may submit a request by **walking into any** PABC **branch** or by **emailing** customerservice@pabcbank.com to exercise your **Right of Access** or **Right to Rectification (modification)**.
- **No DSR form** or prior **DPO approval** is required for these rights.
- A **Branch second officer** will **verify your identity** before processing the request.
- To exercise your Right to Erasure, Right to Withdraw Consent, or Right to Object to Processing, you must complete the Data Subject Rights (DSR) form available on our website.
- Submit the completed form together with supporting documents by email to **dpo@pabcbank.com** .

For Non-Customers and Former Employees

- Complete the DSR (Data Subject Request Form) form available on our website.
- Submit the completed form along with supporting documents via email to **dpo@pabcbank.com** .

For Vendors / Service Providers

- If you are an individual vendor (e.g., sole proprietor, consultant):
  - Complete the DSR form available on our website.
  - Submit the form and supporting documents via email to [DPO email address].
- If you are a corporate entity submitting a request on behalf of an employee:
  - The request must be submitted through the vendor's Data Protection Officer (DPO).
  - The vendor's DPO must complete and submit the DSR form via email from their official corporate email address.
  - A cover letter must be attached, including:
    - Vendor's company name.
    - The employee's full name.
    - The type of request (e.g., access, rectification, deletion).
    - Confirmation that the authorized officer is acting on behalf of the employee.

Identity Verification Requirements

Requestors must provide valid identification documents when submitting a DSR to prevent unauthorized access and ensure compliance with the PDPA.

Required Documents

Requestor Type	Required Documents
Individual (Data Subject Themselves)	One primary ID from Group A.
Former Employee	One primary ID from Group A + proof of past employment (e.g., employee ID, last pay slip, or HR letter).
Vendors / Service Providers	One primary ID from Group A + proof of relationship with the Bank (e.g., vendor agreement).
Third-Party Representative (Legal Representative, Guardian, Heir, or Executor)	One primary ID from Group A + a signed Letter of Authority (LOA) and other legal documents as required.

Accepted Identification Documents

Group A – Primary Identification (Mandatory for All Requests)

- National Identity Card (NIC)
- Valid Passport
- Driver's License

Additional Verification for Special Cases:

- Minors or Incapacitated Individuals – A legal guardian or next of kin must provide a court-issued guardianship order.
- Legal Heirs (Deceased Data Subjects) – Must provide:
    - Death certificate of the data subject.
    - Legal proof of heirship (e.g., probate document or letter of administration).
    - Proof of relationship with the deceased (e.g., birth certificate, marriage certificate, nominee form, or other official document).
- Third-Party Requests (Legal Representative, Guardian, or Executor) – The Letter of Authority (LOA) must:
    - Be signed by the data subject.
    - Include full names and NIC numbers of both the data subject and third party.
    - Specify the rights being exercised (e.g., access, rectification, erasure).
    - Have a validity period of no more than six (6) months from the date of signing.

Processing and Response Timeframes

- Acknowledgment of a request will be sent within 7 working days.
- A formal response will be provided within one month, in compliance with Section 17 of the PDPA.
- Additional time may be required if the request is complex or requires legal consultation.

Special Considerations and Restrictions

1. Joint Accounts and Co-Owned Financial Products

- If a joint account holder submits a request, only their personal data will be provided.

- Any data linked to the co-owner(s) will be redacted unless explicit consent is obtained from all involved parties.

2. Requests from Overseas Data Subjects

- Data subjects residing outside Sri Lanka may submit DSRs via email.
- Additional verification may be required to ensure compliance with local and international data protection laws.

3. Escalation for High-Risk or Exceptional Cases

Some requests may require further review by the PABC Data Protection Committee, including:

- Requests impacting multiple data subjects.
- Requests related to law enforcement or regulatory investigations.
- Requests that conflict with legal obligations or involve sensitive personal data.

We may require additional verification in some cases to ensure the security of your personal data and to prevent unauthorized access.

In some cases, PABC may be legally required to retain your personal data despite your request to withdraw consent. If this applies, we will inform you accordingly and continue to store your data only for the legally mandated retention period.

If you choose to withdraw your consent for the processing of your personal data, please note that:

- PABC may no longer be able to provide you with certain products, services, or account management functions.
- Withdrawal of consent may result in the termination of agreements, restrictions on services, or nullification of contracts with PABC.

We value your privacy and are committed to safeguarding your personal data. We will process your requests promptly and transparently, ensuring that your rights are upheld in accordance with the highest data protection standards, including the PDPA.

For more details on the process or assistance, please refer to the "**Contact Us**" section for the relevant contact details.

15. Reporting Misuse of Personal Data

If you believe that personal data you have provided to the Bank has been misused, lost, or accessed without authorization, you may report this using the Bank's existing complaint handling channels as follows;

- **customerservice@pabcbank.com**
- Messaging option available in Online banking facility
- Messaging option available on the bank website
- Over the phone / through branch

Your complaint will be escalated to the Bank's Data Protection Officer (DPO) for review and appropriate action.

16. CCTV Monitoring

For your safety and to protect our customers, staff, and property, PABC Corporation PLC operates CCTV surveillance at its Head Office and all branch locations across Sri Lanka. This processing is carried out to prevent fraud, ensure security, and support investigations into incidents such as fraud, theft, accidents, security breaches, or violations of laws, regulations, or internal policies.

Where necessary to protect the rights and safety of individuals, or to prevent and detect crime or fraud, CCTV footage may be shared with law enforcement agencies, regulatory authorities, or other legally or contractually authorized third parties, in accordance with applicable laws.

17. Changes to this Privacy Notice

We reserve the right to update or modify this Privacy Notice periodically to:

- Ensure compliance with new or updated legal, regulatory, or industry requirements.
- Reflect changes in our products, services, or business operations, including the introduction of new banking services or technologies.

The latest version of this Privacy Notice will always be available on our website (Privacy Policy Sri Lanka - Pan Asia Banking Corporation). If there are material changes that significantly impact your rights or how we process your personal data, we will notify you through appropriate channels, such as our website, email, or other official communications.

By continuing to use our services after any updates, you acknowledge and accept the revised Privacy Notice. We encourage you to review this notice periodically to stay informed about how we handle your personal data.

18. Contacting Us

If you need assistance regarding your personal data, including:

- Inquiries about your privacy rights, this Privacy Notice, or how your data is handled,
- Exercising your rights under the Personal Data Protection Act, No. 9 of 2022
- Understanding our data retention policies

Please contact our Data Protection Officer (DPO) at **dpo@pabcbank.com** .

If you need to raise a formal complaint regarding the processing of your personal data, please submit it via **dpo.escalations@pabcbank.com** .

Please note that if your Personal Data has been provided to us by a third party, you should contact such party directly to make any queries, feedback, and access and correction requests to PABC on your behalf.

This privacy notice was updated on 01.06.2026.