PRIVACY POLICY

1. Purpose

SANASA Development Bank PLC ("SDB", "we", "our", “us”) is committed to safeguarding your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your personal data in compliance with the Personal Data Protection Act, No. 9 of 2022 (PDPA) of Sri Lanka.

This Policy applies to all personal data collected by SDB bank through its websites, systems, and business operations, and to all individuals whose data we process, including clients, vendors, partners, employees, and visitors.

2. Who We Are

SDB bank is a licensed specialised bank in Sri Lanka that offers customers with a range of competitive financial products and services. We support the national development of Sri Lanka through greater financial inclusion by nurturing SMEs and supporting progressive entrepreneurs through innovation, particularly in rural areas. SDB bank assumes the role of “controller” and “processor” in relation to personal data.

If you have any questions about this Privacy Policy or how your data is processed, you may contact our **Data Protection Officer (“DPO”)** at: **dpo@sdb.lk**.

3. Definitions

For clarity, the terms used in this Privacy Policy follow the definitions set out under the Sri Lankan PDPA:

- **Personal Data**: Any information that can identify a data subject either directly or indirectly, including but not limited to, identifiers like name, financial data, location data, factors specific to the psychological, cultural or social identity of the individual.
- **Data Subject**: An identified or identifiable natural person whose personal data is being processed.
- **Processing**: Any operation on personal data including but not limited to collection, storage, retrieval, use, disclosure, or deletion.
- **Data Protection Officer (DPO)**: The person responsible for overseeing data protection compliance (in accordance with Section 20 of the PDPA).
- **Controller**: For our services, SDB bank is the controller that determines the purposes and means of the processing of personal data.

4. What Personal Data We Collect

The collection and use of your Personal Data has been categorized here based on your relationship with us as follows:

- End Users (our customers using our banking services or products):
    - Identity details (e.g., name, NIC, passport);
    - Contact information (personal address, phone, email);
    - Financial data (account numbers, transactions, balances);
    - KYC and regulatory data (income, employment);
    - Connection details (cookies, IP, device data).

- Business Representatives, Vendors, and Service Providers:
    - Identity details (e.g., name, NIC, passport);
    - Contact information (business address, phone, email);
    - Professional details (job title, company name);
    - Compliance-related information (where legally required, such as KYC/ due diligence).

- Website Visitors:
    - Connection details (cookies, IP, device data);
    - Interaction data (submitted interest forms, user log data).

- Bank Branch Visitors:
    - Identity details (e.g., name, NIC, passport);
    - Biometric data (CCTV surveillance);
    - Service interaction data (meetings notes/ filled forms, complaints, feedback).

- Employees:
    - Identity details (e.g., name, NIC, passport);
    - Contact information (address, phone, email);
    - Professional details (employment history);
    - Biometric or health data (when applicable).

5. How We Collect Your Data

We collect personal data in different ways depending on how you interact with SDB bank:

- End Users:
  - When you first become a customer - for example during onboarding and KYC checks, when opening an account, or when registering for the mobile banking app
  - When you carry out transactions or interact with our digital platforms
  - When our clients provide us access to their systems or user data as part of services we deliver

- Business Representatives, Vendors, and Service Providers:
  - When you enter into contracts or provide services to SDB bank
  - During due diligence, background checks, or compliance processes (e.g., KYC, anti-money laundering checks)
  - Through business communications such as emails, calls, and meetings

- Website Visitors:
  - When you browse our website (e.g., through cookies, log data, or device identifiers)
  - When you submit forms, make inquiries, or contact us via email, phone, branch visits, or online chat

- Bank Branch Visitors:
  - When you enter our premises (through visitor logs or CCTV surveillance for security)
  - When you interact with staff, submit forms, or provide feedback and complaints

- Employees:
  - When you apply for a role with us
  - When you become an employee, as part of HR and compliance processes
  - During your employment, for payroll, benefits, and regulatory purposes.

6. Legal Basis and Purpose for Processing

In line with the Sri Lankan PDPA and other applicable data protection laws, we rely on legal bases to process your Personal Data as follows:

- **Contractual Necessity**: For End Users, we process your personal data when it is necessary to enter into or perform a contract with you. This includes activities such as:
  - Opening and managing your accounts and transactions
  - Providing loans and other financial services
  - Conducting credit and risk assessments
  - Delivering customer support and technical assistance

For Business Representatives/ Vendors, we process data as needed to manage our business relationship, including contracts and compliance obligations.

- **Legal Obligation**: We are required to process certain Personal Data to comply with applicable laws and regulations governing the financial sector. This may include:
    - For End Users:
        - Complying with financial sector laws and regulations such as Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) laws, Know Your Customer (KYC) requirements and tax reporting
        - Managing and monitoring financial transactions to meet regulatory requirements
    - For Business Representatives, Vendors, and Service Providers:
        - Managing client and vendor relationships in line with compliance obligations
        - Fulfilling financial reporting and tax requirements
    - Employees:
        - Administering human resource functions as required by employment and labour laws

- **Legitimate Interest**: We process certain Personal Data where it is necessary for our legitimate interests and only where permitted under the PDPA. This may include:
    - End Users:
        - SDB bank has a legitimate interest in processing your data for risk assessment; fraud detection and prevention; and analytics and improvement of our services and systems.
    - For End Users:
        - Monitoring service usage and improving our platforms, systems and customer experience
        - Conducting analytics to enhance and develop banking services
        - Ensuring system security, including access management and fraud detection/ prevention
    - For Business Representatives, Vendors, and Service Providers:
        - Managing and maintaining client and vendor relationships
        - Ensuring compliance with service standards and operational requirements
    - Employees:
        - Internal monitoring and analytics to improve processes and workplace systems

- **Consent**: We may rely on consent to collect and process Personal Data for optional services, such as:
    - Non-essential cookies on our website or app
    - Marketing communication and promotions
    - Customer surveys, feedback, or service personalization.

You may withdraw your consent at any time, without affecting processing carried out before withdrawal. We would like to note that failure to provide essential data may affect your ability to access certain banking services.

7. Sharing of Personal Data

Your Personal Data is only shared where it is necessary and lawful to do so. This may include sharing your data with:

- Regulatory authorities and law enforcement - to comply with legal and regulatory requirements;
- Financial partners, credit bureaus, CRIB - to meet credit assessment and reporting obligations;
- Auditors, legal advisors, IT vendors and other service providers - these stakeholders help us provide our products and services to you;
- Insurance, card network, and payment partners - to facilitate services such as international remittances, foreign currency transactions and cross-border payments.

We value your trust. That's why we never sell or rent your personal data to others.

8. Cross-Border Transfers

SDB bank primarily serves individuals located in Sri Lanka but certain services - such as international remittances and the use of cloud-based platforms - may involve transferring your Personal Data outside Sri Lanka. Where necessary, we may transfer your data outside Sri Lanka:

- Only to jurisdictions that have an adequate level of data protection, or;
- With adequate safeguards (such as data transfer agreements) in place to protect your data, or
- With binding contracts or your explicit consent, where required.

9. Data Retention and Security

We retain personal data only as long as required for the purposes it was collected or as required by the law. Here are some examples of how long we may keep certain information:

- Legal and contractual data: per statutory limits;
- Marketing data: until consent is withdrawn;
- After retention: data is anonymized or securely deleted.

We seek to align with international standards such as ISO 27001. We take the following measures to ensure protection of your Personal Data:

- Role-based access control
- Encryption of data in transit and at rest
- Secure software development and vulnerability assessments
- Employee confidentiality agreements and data protection training

10. Your Rights Under PDPA

The Sri Lankan PDPA provides you, as a data subject, with rights regarding the collection, use and disclosure of your Personal Data. You may exercise the following rights:

- **Access**: Request access to your Personal Data;
- **Rectification**: Correct inaccuracies or outdated data;
- **Erasure**: Delete data under certain conditions, specifically where processing is no longer lawful;
- **Restriction**: Limit specific processing activities;
- **Objection**: Refuse processing under legitimate interests;
- **Withdraw consent**: Where consent was the legal basis, your consent can be withdrawn at any time

Your rights under the PDPA are consistent with the protections provided to financial consumers under the Central Bank of Sri Lanka's Financial Consumer Protection Regulation (2023).

You may contact our DPO at **dpo@sdb.lk** to exercise your rights. Requests will be handled within 21 working days, with an extension of 14 days made possible on a case-by-case basis for complex cases.

11. Cookies and Tracking Technologies

Some cookies are essential to log you in safely and keep your session active, while others help us remember your preferences or improve how our services work. Our website uses cookies to ensure functionality, analytics to improve our services, and performance. This ultimately helps us keep your online banking experience secure, reliable and smooth.

- Non-essential cookies, such as advertising, will only be set with your consent (you can manage this via our cookie banner).
- You can manage cookie preferences at any time via your browser settings or our consent tool.
- We do not collect sensitive personal data through cookies without your explicit consent.

If you choose to disable cookies, this could limit certain features and affect your overall experience.

12. Automated Decision-Making

We do not conduct automatic decision-making or profiling with legal or similarly significant effects on End Users. However, SDB bank is exploring the use of automated tools, including profiling, for the following purposes:

- Credit scoring, fraud detection, underwriting or transaction monitoring.

If SDB bank adopts automated decision-making that may have significant effects on your person, you will be informed and provided with a right to object or seek human review, express your views, contest the decision and obtain an explanation.

13. Data Breach Notification

In the unlikely event of a personal data breach, we will notify you promptly through your registered contact details (such as SMS, email or in-app alerts) as required by the PDPA. Where required, we will notify regulators and work closely with them to resolve the issue.

Our notification will explain the nature of the data breach, the information that may have been affected, and the steps we are taking to protect you. We will also share recommended security measures and provide regular updates until the issue is resolved.

We are committed to being proactive and transparent in the event of a breach.

14. Third-Party Data Sources

If we collect your Personal Data indirectly, we will:

- Inform you of the source;
- Disclose this at the earliest communication;
- Respect all applicable PDPA notification obligations.

15. Exceptions to Notification

We may not notify data collection when:

- You are already informed;
- Providing notice is impossible or impractical;
- Disclosure is subject to confidentiality or secrecy laws.

16. Policy Review and Updates

We may update this Privacy Policy from time to time to reflect legal or operational changes. The latest version will always be available on our website and our mobile banking app with the updated effective date displayed for your reference.

We may share with you timely disclosures and alerts regarding updates to the Policy or Personal Data collected by contacting you through your SDB bank Dashboard, email address and/ or the physical address registered with SDB bank.

17. Contact Information

If you have any questions or concerns regarding this Policy or your personal data, please contact our DPO:

Data Protection Officer
SANASA Development Bank PLC
Email: **dpo@sdb.lk**
Phone: +94 11 5411 411
Address: No. 12, Edmonton Road, Kirulapone, Colombo 06