

Privacy Notice

Version 1.0

Last updated: 24.11.2025

This Privacy Notice applies to the processing of personal data by **First Capital Holdings PLC** and its subsidiaries (“First Capital”, “Company”). We are committed to protecting your personal data and processing it in accordance with the Personal Data Protection Act No. 9 of 2022 (“PDPA”) and other applicable laws in Sri Lanka.

We act as **Data Controller** (and in certain cases **Data Processors**) for the personal data collected and processed in connection with our services.

Scope of this Notice

The notice covers personal data collected and processed in connection with our client and investment services, digital onboarding and account opening, website and portal usage, marketing and communications, employment and recruitment activities, vendor and contractor engagements, and the management of access to our premises. Through this notice, we aim to ensure transparency in how we handle personal data across all interactions with individuals and entities connected to our business.

Depending on your relationship with us as a **customer/client, employee/director/shareholder or job applicant, or visitor, contractor, or vendor**, different sections of this Notice will apply.

A. CUSTOMERS / CLIENTS / INVESTORS

Data Types

We may collect the following types of data from you depending on the service you use, and the interactions you have with us:

- Identity and Contact Data
 - Full name, title, national identification card number or passport number, date of birth, nationality, gender, citizenship
 - Contact details (address, email, phone / fax numbers)
 - Bank account details
 - Tax Identification Number (TIN) or other tax-related identifiers
 - Details of Nominee
- Financial Transactional Data
 - Details of investments, trades, transactions, portfolio holdings, and financial statements
 - Payment records, dividends, interest, and capital movements
 - Payment instructions, deposit/withdrawal data
- Compliance and Regulatory Data

- Know Your Customer (KYC) information: status of residence / employment details / source of funds / anticipated monthly volume , Politically Exposed Person (PEP) status, Foreign Account Tax Compliance Act (FATCA) classification
 - Sanctions screening and Anti-Money Laundering (AML) verification results
 - Risk profiling data
- Sensitive / Special-Category Data (only where required)
- Biometric data (facial/video verification for e-boarding) processed only with explicit consent and additional safeguards

Why we Collect and Process

We process customer data to:

- Provide and manage our financial, investment, or advisory services
- Conduct identity verification (KYC/Customer Due Dilligence)
- Fulfil legal and regulatory obligations (e.g., AML, CBSL, SEC)
- Communicate account statements, transaction confirmations, and notifications
- Improve our services, systems, and user experience
- Comply with tax laws and reporting
- Send marketing communications

Data Sharing

We may share your data with:

- Group companies for consolidated client service and operations
- Regulatory authorities
- Third-party custodians, brokers, or IT/onboarding service providers under contractual safeguards
- Auditors, legal advisors, or other entities as required by law
- Overseas entities (cross-border transfers) under PDPA-compliant safeguards

Retention

Your personal data will be retained:

- As long as you remain a client, and
- For the period required by applicable laws, regulations, and internal policies (including statutory record retention periods).

Data will be securely deleted or anonymized once retention requirements expire.

B. EMPLOYEES / DIRECTORS / SHAREHOLDERS AND JOB CANDIDATES

Data Types

- For Job Applicants:
 - Identity and contact information (name, NIC/passport, contact details)
 - Educational qualifications, CV/resume details provided on personal interest, references, background check results
 - Interview records and assessments
- For Employees (current and former) / Directors / Shareholders / Ultimate Beneficial Owners:
 - Employment details: designation, employee number, department, work location, attendance, performance records
 - Salary and other remuneration details
 - Bank and tax details
 - Health and emergency contact details (for occupational safety/welfare)
 - CCTV footage, access-control logs, company email (for IT security and compliance monitoring)
 - Personal information of related parties
- Sensitive Data (only where necessary):
 - Bio-metric details (photos and fingerprints)
 - Medical or disability information (for insurance or health-and-safety purposes)
 - Disciplinary or grievance records
 - Background verification or police reports
 - Investment / transactional details / shareholding details
 - Organizational structures

Why we Collect and Process

- Recruitment, selection and pre-employment verification
- Employment contract administration (payroll, benefits, performance, insurance)
- Compliance with labour, tax and social-security laws
- Corporate governance, audit, and HR record-keeping
- Health, safety and security of our employees and premises
- IT/network security, access control and internal investigations
- Processing of share dividend / coupon payments of debentures
- Financial reporting
- Reporting of ultimate beneficial owners / maintaining shareholder database

Data Sharing

We may share your data with:

- Payroll and benefits providers, insurers, medical service providers
- Government and regulatory authorities (e.g., IRD, EPF/ETF, Labour Department, CBSL, SEC)

- IT, HR, and recruitment vendors who act as data processors under confidentiality agreements
- Auditors or consultants under confidentiality agreements

Retention

- **Employees:** Data is retained for the duration of employment, and the personal data of resigned employees is preserved in accordance with applicable labor and tax law requirements
- **Job Applicants:** For job applicants, personal data is retained throughout the recruitment process and remains in the candidate database for a period of one year for consideration in future job opportunities

C. VISITORS, CONTRACTORS & VENDORS

Data Types

- Visitors:
 - Name, identification document, contact details, organizational details, visit purpose, date/time of visit
 - CCTV footage, access logs, vehicle number, and temperature/health details (if required for safety)
- Contractors and Vendors:
 - Company details authorized personnel contact information, NIC/passport copies (for access or verification).
 - Business registration, bank account details, tax registration (including TIN), compliance documents.
 - Performance records, communications, and payment data.

Why we Collect and Process

- Premises access control and physical security
- Vendor/contractor onboarding, due diligence and payment processing
- Health and safety monitoring
- Compliance with procurement, anti-corruption, and AML requirements

Data Sharing

We may share such data with:

- Security service providers managing access control and CCTV systems
- Auditors, regulatory authorities or law enforcement (if required)
- Group companies and relevant business units for vendor management

Retention

- **CCTV:** remained for 6 months unless required for investigations
- **Visitor logs :** remained for 6 months unless required for investigations
- **Vendor/contractor data:** retained until contract termination or for the period mandated by applicable financial and audit regulations, based on the lawful basis of contract execution

GENERAL INFORMATION

Your Rights

Under the PDPA, you have the following rights (subject to applicable exemptions and conditions):

- **Right of access** - You may request access to your personal data that we hold
- **Right to rectification or completion** - If your data is inaccurate or incomplete you may request correction or completion
- **Right to erasure (right to be forgotten)** - Under certain conditions you may request deletion of your data
- **Right to withdraw consent or object** - You may withdraw your consent or object to processing (where we rely on consent or legitimate interest).
- **Right in relation to automated decision-making / profiling** - Where we use automated decision-making (including profiling) you have the right to request explanation and human review
- **Right to data-portability or transfer** - Where applicable you may request your data in a structured, commonly used, machine-readable format and transfer to another controller (subject to conditions)
- **Right to lodge a complaint** with the Data Protection Authority of Sri Lanka or other supervisory authority.

To exercise any of these rights please contact us. We may ask you to verify your identity before responding to your request. We endeavor to respond without undue delay and in compliance with legal time frames.

Cookies and tracking technologies

When you use our website, we may place cookies or similar technologies to track your activity, gather analytics, enhance user experience and provide our services. You will be provided with a cookies-banner or settings allowing you to consent to or manage non-essential cookies. Essential cookies (necessary for operation of the website) will be placed without consent because of our legitimate interest.

We use Google Analytics to better understand how visitors interact with our website and to improve its performance, content, and user experience. Google Analytics collects information such as your IP address, device type, browser information, pages visited, time spent on pages, and

referring websites. This information is collected through cookies and similar tracking technologies. Google may process this data on our behalf and may store it on servers located outside Sri Lanka. We do not use Google Analytics to identify individuals, nor do we combine analytics data with other personally identifiable information. You can manage or disable cookies through your browser settings. You may also opt out of Google Analytics by using Google's opt-out tool.

Security and Data Protection

We take appropriate technical and organizational measures to protect personal data against unauthorized or accidental access, disclosure, alteration or destruction. These measures include secure servers, encryption, logical access controls, regular audit and monitoring, vendor-due-diligence and incident-response procedures. We also require our service providers to implement equivalent measures. In the event of a personal data breach that is likely to result in high risk to your rights and freedoms, we will notify the Data Protection Authority and affected individuals as required by law.

International Transfers

If your personal data is transferred to or processed in a jurisdiction outside Sri Lanka, we will ensure appropriate safeguards are in place (for example standard contractual clauses, binding corporate rules, or if the jurisdiction is designated adequate). We will inform you as required by law.

Children and Minors

Our services are primarily designed for adults (18 years and above) in Sri Lanka. However, we may provide certain services or accounts to minors with the valid consent of a parent or legal guardian. We do not knowingly collect personal data from minors without such consent. If you believe that a minor's personal data has been provided to us without the required authorization, please contact us so that we may delete the data or obtain the appropriate consent.

Contact Us

If you have any questions about this Privacy Notice, or wish to exercise your rights, you may contact our Data Protection Officer (DPO):

Name: Ms. Devindee Tissera

Email: devindee@firstcapital.lk | RiskCompliance@firstcapital.lk

Voice: 011 2639895

Postal address: No. 02, Deal Place, Colombo 00300, Sri Lanka.

We will endeavor to respond to your request without undue delay and within the time frames required by law.

If you are not satisfied with our response, you may escalate the complaint to:

Data Protection Authority of Sri Lanka,

1st Floor, Building No. 5, BMICH Premises, Bauddhaloka Mawatha, Colombo 07.