

CAIRO BANK UGANDA LIMITED**Data Privacy Statement**

1. About this Statement

This Data Privacy Statement ("Statement") explains how Cairo Bank Uganda Limited ("CBUL", "the Bank", "we", "us" or "our") collects, uses, shares, protects and keeps personal data, and the rights you have over your personal data.

It is issued in line with Article 27 of the Constitution of the Republic of Uganda, 1995 (right to privacy), the Data Protection and Privacy Act, Cap. 97 ("the Act"), the Data Protection and Privacy Regulations, 2021 ("the Regulations"), and CBUL's Board-approved Data Protection and Privacy Framework.

Please read this Statement together with the applicable terms and conditions governing the products and services you use. In the event of any inconsistency relating to the collection, use, storage, disclosure, or otherwise processing of personal data, this Statement shall prevail to the extent of such inconsistency, unless otherwise required or permitted by applicable data protection and privacy laws and regulations.

2. Who we are

CBUL is a commercial bank licensed and regulated by the Bank of Uganda, and a subsidiary of Banque du Caire.

For most of the personal data described in this Statement, CBUL is the data controller. This means we decide why and how your personal data is processed, and we are accountable to you for it. CBUL is registered with the Personal Data Protection Office (PDPO), registration number: PDPO-202201-0060.

Registered office and postal address:

- Arie Towers,
- Plot no. 16, Mackinnon Road - Nakasero.
- Ground, First and Ninth Floor.
- P.O. Box 7052, Kampala – Uganda.

3. Who this Statement applies to

This Statement applies to individuals (natural persons) whose personal data we process, including:

- Customers and prospective customers, including joint account holders and anyone who applies for, uses or enquires about our products and services.
- Persons connected with a customer, such as authorised signatories, attorneys, parents and guardians, next of kin, guarantors, sureties, payment beneficiaries and beneficial owners.
- Directors, shareholders, officers, beneficial owners and representatives of our corporate and institutional customers, suppliers and agents.
- Banking agents, merchants and their staff.
- Suppliers, service providers, external lawyers, valuers, auctioneers and other professional service providers, and their personnel.
- Job applicants and CBUL directors.
- Visitors to our branches, offices and ATM locations.
- Users of our website, internet banking, mobile banking and other digital channels.
- Bank current and former Employees.

Companies and other legal entities are not data subjects. However, this Statement applies to the personal data of the individuals connected with them.

This Statement covers personal data in any form (electronic, paper or oral). It continues to apply after your relationship with us ends, for as long as we hold your personal data.

4. Key terms

- **Personal data:** Information about a person from which that person can be identified, in any form. Examples include name, identification number, nationality, age, marital status, occupation, contact details and opinions expressed about the person.
- **Special personal data:** Under the Act, personal data relating to religious or philosophical beliefs, political opinion, sexual life, financial information, health status or medical records.
- **Processing:** Any operation on personal data, automated or not, including collection, storage, use, disclosure, combination, blocking, erasure or destruction.
- **Data controller:** The person who decides the purposes for which, and the manner in which, personal data is processed.
- **Data processor:** A person (other than an employee of the data controller) who processes personal data on the data controller's behalf, such as an outsourced service provider.
- **Consent:** A freely given, specific, informed and unambiguous indication of your wishes, by a statement or clear affirmative action.
- **PDPO:** The Personal Data Protection Office, established under the Act within the National Information Technology Authority – Uganda (NITA-U), which oversees data protection in Uganda.

5. Our data protection principles

In line with the Act, we are accountable to you for the personal data we hold, and we:

- Collect and process personal data fairly and lawfully, on a lawful basis.
- Collect only data that is adequate, relevant and not excessive for the purpose (see Section 9).
- Keep personal data only as long as the law allows or the purpose requires.
- Take reasonable steps to keep it complete, accurate and up to date.
- Tell you how your data is used and enable you to take part in decisions about it.
- Protect it with appropriate security safeguards.

6. Personal data we collect

We collect different data depending on your relationship with us. Not every category applies to everyone.

Category	Examples
Identification	Full name, title, photograph, date of birth, age, sex, nationality, National Identification Number and card, passport or other travel document, driving permit, alien or refugee identification, birth certificate number (for minors), specimen signature
Contact	Residential, physical and postal address, telephone numbers, email address, social media handles only where you choose to interact with us on social media
Due diligence (KYC and AML/CFT)	Occupation, nature of business, source of funds and wealth, politically exposed person status where required by law, sanctions screening results, beneficial ownership, results of identity verification checks
Financial and banking	Account numbers and balances, card details, loans and repayment history, collateral and security details (including property details and valuations)
Transaction	Payments, transfers, deposits and withdrawals, beneficiary and remitter details, channel, date, time and location of the transaction (branch, ATM, agent or digital)
Credit	Credit applications, credit reports and scores from licensed credit reference bureaus, repayment conduct, defaults

Category	Examples
Employment and income	Employer, terms and expiry of employment contract, estimated monthly income, for students, institution and expected graduation date
Biometric	Fingerprints and facial images used to identify and authenticate you.
Images and recordings	CCTV footage, photographs and videos at CBUL events, recorded telephone calls.
Communications	Letters, emails, WhatsApp and social media messages, complaints, feedback and survey responses
Digital, device and technical	IP address, device identifiers, device model and operating system, browser type, cookie identifiers, log-in and usage records on our website and apps
Location	Location of branches, ATMs and agents where you transact, location of property or business premises for credit and climate-risk assessment, device location in our apps.
Premises and visitors	Name, organisation, telephone number, National ID number, vehicle registration, serial numbers of devices you bring onto our premises, parking requests
Connected persons	For guarantors, next of kin, beneficiaries, directors, shareholders and beneficial owners: names, identification numbers, nationality, date of birth, addresses, contact details, occupation, nature of ownership or control, shareholding
Environmental and social due diligence	Information about a borrower's operations, and the individuals who own or manage them, needed to assess environmental, social and climate-related risk
Preferences	Product interests, marketing preferences and consent records

Special personal data. The Act classifies **financial information** as special personal data. Because handling financial information is central to banking, we process it only where needed to provide the services you ask for, to comply with the law, or with your consent, and we protect it as confidential information.

We collect health or medical information only where the law requires or permits it (for example, to record and report accidents and incidents on our premises) or with your consent.

Biometric data is not special personal data under the Act, but we give it the same level of protection.

Children. A child is a person below 18 years of age. We collect and process a child's personal data only with the prior consent of a parent, guardian or other person with authority to decide on the child's behalf, or where the law requires or permits it (including for research or statistical purposes). For products for minors, we verify age and record the parent's or guardian's consent. We process children's data in a way that protects the child's rights and best interests. A parent or guardian may exercise the child's rights under Section 23 on the child's behalf.

7. How we collect personal data

Directly from you: When you apply for, use or enquire about our products and services at a branch, through an agent or merchant, at an ATM, through internet or mobile banking, on our website (<https://cbu.co.ug>), by email, by telephone, on WhatsApp or social media, when you visit our premises, attend a CBUL event, respond to a survey, apply for a job or offer services to us.

Automatically: Through CCTV, call recording, transaction records, and cookies and similar technologies on our digital channels.

From third parties: Where the law permits, including: licensed credit reference bureaus, government databases used to verify identity, public registers, your employer, guarantor or authorised

representative, other banks, correspondent banks and payment systems, fraud-prevention and law-enforcement bodies, and regulators.

We collect personal data directly from you wherever practicable. When we ask for information, we tell you whether it is mandatory or optional and what happens if you do not provide it. For example, we cannot open an account without the identification information that anti-money laundering law requires.

8. Why we use personal data and our lawful basis

We process personal data only where we have a lawful basis. **Consent is one basis, but not the only one.** Much of our processing is necessary to perform our contract with you or to comply with the law and does not depend on your consent.

The lawful bases we rely on are:

- **Contract:** To perform a contract with you, or to take steps you ask for before entering into one.
- **Legal obligation:** To comply with the law, including the Financial Institutions Act, anti-money laundering and counter-terrorist financing laws, tax laws and Bank of Uganda requirements, or where processing is otherwise authorised or required by law.
- **Prevention of offences:** To prevent, detect, investigate or prosecute an offence or breach of law.
- **Legitimate interests:** Processing you would reasonably expect, or for which there is a compelling justification, such as preventing fraud, maintaining network and information security, preventing crime and internal administration. We must be able to show that the interest is legitimate.
- **Consent:** Where you have given it, for example for marketing.
- **Other bases in the Act,** where they apply, national security, the proper performance of a public duty by a public body, and medical purposes.

Purpose	Main lawful basis
Account opening, onboarding and identity verification	Contract, legal obligation.
Customer due diligence, AML/CFT, sanctions and politically exposed person screening, suspicious transaction reporting.	Legal obligation, prevention of offences.
Providing products and services: accounts, payments, cards, digital and agent banking.	Contract.
Credit assessment, lending, credit scoring and collateral valuation	Contract, legal obligation.
Sharing and obtaining credit information with licensed credit reference bureaus.	Legal obligation.
Recovery, collections and enforcement of our rights	Contract, legitimate interests, authorised by law.
Fraud prevention, detection and investigation	Prevention of offences, legitimate interests, legal obligation
Risk management, including environmental, social and climate-risk assessment	Legal obligation, legitimate interests
Regulatory, statutory and tax reporting	Legal obligation
Responding to lawful requests from courts, regulators and law enforcement	Legal obligation
Customer service, queries and complaints	Contract, legal obligation, legitimate interests.
Recording calls to verify instructions, resolve disputes and maintain service quality	Legitimate interests.

Purpose	Main lawful basis
Physical security, CCTV, visitor registers and access control	Legitimate interests, prevention of offences.
Cybersecurity and protection of our systems	Legitimate interests, legal obligation.
Business continuity and disaster recovery	Legal obligation, legitimate interests.
Internal audit, external audit and assurance	Legal obligation, legitimate interests.
Improving products and services, statistics and research (de-identified wherever possible)	Legitimate interests, consent where required.
Marketing and market research	Consent.
Photographs and videos at CBUL events used for publicity	Consent.
Recruitment and records of directors	Contract, legal obligation, consent for background checks where required
Due diligence on, and payment of, suppliers, agents and professional service providers	Contract, legal obligation, legitimate interests.
Sale, merger or transfer of any part of our business	Legitimate interests, authorised by law, subject to confidentiality.
Recording and reporting accidents and incidents on our premises	Legal obligation

We use personal data for a new purpose only if it is compatible with the purpose for which it was collected, or if another lawful basis applies.

9. Data minimisation | we collect only what we need

CBUL collects and processes only personal data that is **adequate, relevant, necessary and proportionate** for the specific and lawful purpose for which it is processed, and not excessive. In practice:

- We ask only for the information needed for the product, service or legal requirement concerned.
- We tell you which information is mandatory and which is optional.
- We design new products, systems and processes to collect only the data needed, by default.
- Where a purpose can be met with anonymised or aggregated data, we use that instead.
- Our staff and service providers can access personal data only where they need it for their role.

Some laws require us to collect specific information, such as identity and source-of-funds information under anti-money laundering law. In those cases, the information is necessary for us to meet our legal obligations.

10. Consent and withdrawing consent

When we ask for consent: For example, for marketing, optional product features, non-essential cookies, publicity use of event photographs, a transfer outside Uganda where the destination does not have adequate protection, and the personal data of children (from a parent or guardian).

What valid consent means: Your consent must be freely given, specific, informed and unambiguous, and given by a clear statement or action. We keep a record of the consents you give.

How to withdraw consent: You may withdraw consent at any time through any of the channels in Section 25. You may also use the PDPO's prescribed Form 1 (Notice of Objection to Collection/Processing of Personal Data). We will act on your withdrawal as soon as practicable after verifying your identity.

What withdrawal means:

- It does not affect processing carried out before you withdrew.
- It may mean we can no longer provide a product or feature that depends on that consent, and we will tell you if so.
- It does not stop processing we carry out on another lawful basis, such as keeping records that anti-money laundering law requires or performing a contract you have with us.

11. Keeping your data accurate

We take reasonable steps to keep your personal data complete, accurate and up to date, including by periodically asking you to update your due diligence information.

You are responsible for giving us accurate and complete information and for telling us promptly of changes, such as a new address, telephone number, name or employer. Giving false or misleading information may lead us to decline or end a service and may be an offence under applicable law.

If you give us information about another person (for example, a guarantor, next of kin or payment beneficiary), please make sure you are entitled to do so and let that person know about this Statement.

12. Credit scoring, profiling and automated decisions

We use credit scoring and analysis of your information (including your application, account conduct and credit reference reports) to assess creditworthiness and affordability, and to manage fraud and financial-crime risk.

Except for creditworthiness in case of borrowing for some digital loan applications, there will be no decision that significantly affects customers, is taken solely by automated means.

Where a decision that significantly affects you is based solely on automated processing, we will tell you as soon as reasonably practicable. You may, by written notice, require that such a decision is not based solely on automated processing, or ask us to reconsider it. We will reply in writing within 14 days, stating whether we have complied or intend to comply, or our reasons if we do not. If we do not comply, the PDPO may direct us to do so.

13. Marketing and communications

With your consent, we may contact you about CBUL products, services, offers, events and market research by SMS, email, telephone or WhatsApp.

You can object to direct marketing, or withdraw your consent, at any time through any channel in Section 25 or by using the opt-out option in the message. We will reply in writing within 14 days and stop using your data for direct marketing. If we tell you that we intend to continue, you may ask the PDPO in writing, within 14 days, to review our decision.

You cannot opt out of messages we must send to operate your account or to comply with the law, such as security alerts, statutory notices and notices of changes to your terms and conditions.

CBUL does not sell your personal data.

14. CCTV, call recording, premises and events

CCTV operates in our branches, offices and ATM locations for the safety of customers and staff and to prevent and detect crime. Access to footage is restricted, and footage is kept for a limited period of 6 months unless it is needed for an investigation or legal proceedings.

Telephone calls to and from CBUL may be recorded to verify instructions, resolve disputes and maintain service quality. We will tell you when a call may be recorded.

Visitors and parking. We keep a visitor register and parking records for security, health and safety purposes.

Accidents and incidents. If you are involved in an accident or incident on our premises, we record the details and, where the law requires, report them to the relevant authority. We review incidents on an anonymised basis to prevent recurrence.

Events. We may take photographs and videos at CBUL events for publication. We will tell you at the event. If you do not want to be photographed or featured, please tell our event staff or contact us.

15. Cookies and digital channels

Our website (<https://cbu.co.ug>), internet banking, mobile banking app and other digital channels use cookies and similar technologies. Cookie identifiers, IP addresses and device identifiers can identify you, and we treat them as personal data.

We use:

- **Strictly necessary** cookies, for security, log-in and fraud prevention.
- **Functional** cookies, to remember your preferences.
- **Analytics** cookies, to understand how our channels are used and improve them.

You can manage cookies through your browser settings. Blocking strictly necessary cookies may stop parts of our channels from working.

Our apps may ask for device permissions, such as the camera to capture identity documents, or notifications. You can manage these permissions in your device settings.

Our website may link to other websites, and we may interact with you on third-party social media platforms. Their own privacy policies apply. Please do not share account details, PINs or passwords on social media.

16. Who we share personal data with

We share personal data only where there is a lawful basis and a specific, legitimate purpose, only the data necessary for that purpose is shared, and the recipient is bound in writing to keep it confidential and secure. Subject to these safeguards, we may share personal data with:

- The **Bank of Uganda** and other regulatory and supervisory authorities, the Financial Intelligence Authority, the Uganda Revenue Authority and other government bodies, where the law requires or permits.
- **Courts, tribunals, arbitrators and law-enforcement agencies**, in response to a lawful demand;
- **Licensed credit reference bureaus**, as required or permitted under Bank of Uganda credit reference regulations.
- **Payment systems, card schemes, SWIFT, correspondent banks and other financial institutions**, to carry out your transactions.
- **Service providers** acting on our behalf, such as IT, core banking, cloud, card production, printing, archiving, call-centre and debt-collection providers (see Section 17).
- **Banking agents and merchants**, to provide services at their locations.
- **Professional advisers**, including external lawyers, valuers, auctioneers, auditors and insurers or brokers;
- **Banque du Caire and other members of our group**, for consolidated reporting, group risk management, audit and financial-crime compliance, subject to Section 18.
- A prospective buyer, transferee or assignee of any part of our business or assets, under confidentiality obligations.
- Persons you authorise, such as an attorney or representative.
- Other persons where the law requires or permits disclosure, including to protect CBUL, our customers or others from fraud or crime.

We may share aggregated or de-identified information, which does not identify you, for research and statistical purposes.

17. Service providers (data processors)

When we engage a service provider to process personal data for us:

- We carry out due diligence, including on privacy and security, before appointment.
- The provider must process the data only on our instructions and keep it confidential.
- The contract requires security measures at least equivalent to our own, controls on any sub-processors, audit rights, prompt notice to CBUL of any breach, agreed data locations, and return or secure deletion of data when the service ends.
- We review the arrangement at least annually.

These controls operate under our Third-Party Risk Management and Outsourcing Policy and Cloud Risk Management Framework. CBUL remains accountable for your personal data when a service provider processes it for us.

18. Transfers outside Uganda

Some processing may take place outside Uganda, for example:

- To carry out international payments through SWIFT, correspondent banks and card schemes.
- For group reporting and oversight by our parent company in Egypt.
- Where a service provider hosts or supports our systems outside Uganda.

We process or store personal data outside Uganda only where the destination country has adequate data protection measures, at least equivalent to those under the Act, or where you have consented.

Where we rely on consent, we will explain the purpose and nature of the transfer, including any onward transfer. Personal data transferred outside Uganda is not transferred on to another country without your express consent. For purpose of this requirement, the consent obtained for the initial transfer shall expressly extend to and cover any subsequent or onward transfer of personal data to another third country provided that the data subject has been clearly transparently informed of the possibility, purpose and nature of such further transfer at the time consent is obtained.

When you instruct an international payment, the payment details must pass to the banks and intermediaries in the payment chain to carry out your instruction.

We keep a record of our cross-border data flows and protect them with contractual and security safeguards.

19. How we protect your personal data

We use appropriate, reasonable technical and organisational measures to protect personal data against unauthorised access, loss, damage, destruction, alteration, disclosure, misuse and other unlawful processing. These include:

- Access limited to authorised persons on a need-to-know basis;
- Authentication, encryption where appropriate, and monitoring of our systems and networks;
- Physical security at our premises;
- Confidentiality undertakings and data protection training for staff;
- Security requirements for our service providers; and
- Regular testing and review of our controls.

We follow generally accepted information security practices and any security practices published by the PDPO. We do not publish detailed security arrangements, as doing so could put your data at risk.

Your part. Keep your PIN, passwords and one-time codes secret. CBUL will never ask you for your PIN, full password or one-time code. Report suspected fraud or unauthorised access immediately on 0800 211 025 (Toll Free) or reportfraud@cbu.co.ug or whistleblow@cbu.co.ug

20. If a data breach happens

If personal data is lost, or accessed or disclosed without authorisation, we act promptly to contain the incident, investigate it and assess the risk to the people affected.

Where personal data has been accessed or acquired by an unauthorised person, we notify the PDPO immediately, as the law requires. Where the PDPO determines that affected individuals should be notified, we will inform you by registered mail, email, a prominent notice on our website or publication in the media, as directed. We will give you enough information to take steps to protect yourself.

We record every incident and act on the lessons learned. If you suspect that your personal data held by CBUL has been compromised, please contact us immediately (Section 25).

21. How long we keep personal data

We keep personal data only as long as necessary for the purpose for which it was collected, unless longer retention is:

- Required or authorised by law;
- Necessary for a lawful purpose connected with our functions;
- Required by a contract; or
- Agreed to by you.

We may also keep data for longer to prevent, detect or investigate offences, for court proceedings, to enforce tax and revenue laws, or for historical, statistical or research purposes (de-identified wherever possible).

Retention periods are set in CBUL's Data Retention Schedule, taking into account the length of your relationship with us, statutory record-keeping requirements (including anti-money laundering, tax and Bank of Uganda requirements), and limitation periods for legal claims.

At the end of the retention period, we securely destroy, delete or de-identify personal data so that it cannot be reconstructed. Archived records remain protected for as long as we hold them.

22. Confidentiality

We keep your personal and account information confidential in line with the banker's duty of confidentiality and applicable law, including the Financial Institutions Act. Our staff and service providers are bound by confidentiality obligations. We disclose personal data only as described in Section 16. Our duty of confidentiality continues after your relationship with us ends.

23. Your rights

Subject to the conditions and exceptions in the law, you have the following rights.

Right	What it means	How to exercise it	Our response
To be informed	To know that we are collecting your personal data, why, and who will receive it	This Statement and notices at the point of collection	Before or, where the law permits, as soon as practicable after collection
To access	To ask whether we hold personal data about you, and for a description and copy of it	Written request (you may use PDPO Form 8) with proof of identity: national or alien identification card, passport or travel document, or driving permit	We will tell you our decision within 7 days, with reasons if we refuse
To correct or delete	To ask us to correct or delete data that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained, or to destroy data we are no longer authorised to keep	Written request	We will tell you our decision in writing within 7 days. If we make a correction, we will inform those to whom we disclosed the data. If we refuse, we will give reasons

Right	What it means	How to exercise it	Our response
To rectify, block, erase or destroy inaccurate data	To have inaccurate data rectified, blocked, erased or destroyed	Written request	If we do not comply within 30 days, you may complain to the PDPO using Form 9
To withdraw consent or object	To withdraw consent, or object to processing based on consent	Any channel in Section 25, or PDPO Form 1	As soon as practicable after verifying your identity (see Section 10)
To prevent processing	To require us to stop processing that is not compatible with the purpose for which the data was collected, or that is likely to cause you unwarranted substantial damage or distress	Written notice	We will reply in writing within 14 days. If we do not comply, we will give reasons and copy our reply to the PDPO within 7 days
To object to direct marketing	To require us to stop using your data for direct marketing	Any channel in Section 25	We will reply in writing within 14 days and stop (see Section 13)
On automated decisions	To require that a decision significantly affecting you is not based solely on automated processing	Written notice	We will reply in writing within 14 days (see Section 12)
To complain	To complain to CBUL and to the PDPO	See Section 24	See Section 24

Limits on rights. These rights are not absolute. We may decline or limit a request where complying would prejudice the prevention, detection, investigation or prosecution of an offence, national security, the enforcement of tax or revenue laws, or court proceedings, or where the law (such as anti-money laundering record-keeping) requires us to keep or continue processing the data. We will explain our reasons in writing, unless the law prevents us from doing so.

Verification and representatives. We will verify your identity before acting on a request. Someone may act on your behalf with proof of their authority.

24. Complaints and escalation to the PDPO

Step 1: Contact CBUL. If you are concerned about how we handle your personal data, please contact our Data Protection Officer at dpo@cbu.co.ug or use any channel in Section 25 or visit any branch. Please give your name, contact details, account number (if any), a description of your concern and the outcome you are seeking. We will acknowledge and respond to your complaint. We record every complaint.

Step 2: Complain to the PDPO. If you are not satisfied with our response, or at any time you believe CBUL is infringing your rights or the Act, you may complain to the **Personal Data Protection Office**, addressed to the National Personal Data Protection Director. The Regulations prescribe these forms:

- **Form 11** — complaint about infringement or violation of the Act;
- **Form 9** — complaint about inaccurate personal data held by a data controller; and
- **Form 6** — complaint about processing without appropriate security measures.

PDPO contact: info@pdpo.go.ug or via the PDPO website: <https://pdpo.go.ug>

Step 3: Appeal. If you are dissatisfied with the PDPO's decision, you may appeal to the Minister responsible for information and communications technology within 30 days of the decision, using Form 13 addressed to the Permanent Secretary of that Ministry, with a copy to the PDPO.

We encourage you to contact us first so that we can try to resolve your concern quickly, but you do not have to. These routes do not affect any other legal remedy available to you.

25. Data Protection Officer and Contact Us | Data Protection and Privacy Enquiries

CBUL has designated a **Data Protection Officer (DPO)** under the Act and the Regulations. The DPO is CBUL's point of contact with the PDPO, responds to data subjects, ensures that requests to access or erase personal data are handled, and monitors CBUL's compliance with the Act.

For any data protection or privacy question, request or complaint, contact us through:

Channel	Details
Bank website	https://cbu.co.ug
Email1	dpo@cbu.co.ug
Email2	feedback@cbu.co.ug
Telephone	0800 211 025 (Toll Free)
WhatsApp	0786 650 966
Postal / physical address	P.O. Box 7052, Kampala – Uganda. Head Office location: Arie Towers, Plot no. 16, Mackinnon Road - Nakasero. Ground, First and Ninth Floor.

Please mark written requests "Data Protection" so they reach the DPO without delay.

26. Our accountability

CBUL's approach to personal data is governed by a Board-approved Data Protection and Privacy Framework, overseen by the Board Risk Committee and the Executive Committee. Our DPO monitors compliance, and our Internal Audit function provides independent assurance.

We maintain records of our processing activities, consents, data subject requests, complaints, data breaches and data-sharing arrangements. We carry out data protection impact assessments before processing that poses a high risk to individuals. We train our staff on data protection.

We renew our registration with the PDPO as required, and we report to the PDPO annually on the complaints we receive and any data breaches, and the action taken.

27. Changes to this Statement

We review this Statement at least once a year, and sooner if the law or our practices change. The current version, with its effective date, is published at <https://cbu.co.ug>.

Where we make a material change, we will tell you before it takes effect where reasonably practicable notification channels, e.g. website, branch notices, SMS or email. A change to this Statement does not reduce your rights under the law. Where a change requires your consent, we will ask for it.

28. Document Control

Field	Detail
Document title	Cairo Bank Uganda Limited – Data Privacy Statement
Document owner	Data Protection Officer (Framework s.15.0 and s.38.0)
Document custodian	Data Protection Officer, in conjunction with Risk Management

Field	Detail
Approval authority	Recommendation by the DPO, Approval by Bank's Executive Committee with notification to the Board Risk Committee. The CBUL Board of Directors retains ultimate authority and responsibility for this Statement.
Effective date	30 September 2026
Version number	2.0
Review frequency	At least annually, or earlier on a material change in law, regulation or CBUL practice.
Next review date	August 2027
Classification	Public
Supersedes	All earlier versions
Related documents	Data Protection and Privacy Framework, Information Security Policy, Information Classification Policy, Third-Party Risk Management and Outsourcing Policy, Cloud Risk Management Framework, Records Management Policy, Data Retention Schedule, Enterprise Risk Management Framework, Agent Banking Risk Management Framework, product terms and conditions.
Regulatory basis	Constitution of the Republic of Uganda, 1995 (Art. 27), Data Protection and Privacy Act, Cap. 97, Data Protection and Privacy Regulations, 2021 (S.I. No. 21 of 2021), PDPO guidance and prescribed forms, Financial Institutions Act, Anti-Money Laundering Act, Bank of Uganda requirements.

APPROVED SET