



PRIVACY STATEMENT 2025

PRIVACY STATEMENT

Your privacy is important to us. This privacy notice explains the personal data Family bank collects, how it is processed, for what purposes and how you can exercise your rights in relation to processing of personal data.

1. DEFINITIONS

"FBL", "We," "our," "ours," and "us," means Family Bank Limited, Family Group and includes its successors in title and assigns, its affiliates and/or its subsidiaries as may from time to time be specified by the Bank to you.

You means;

- a) Customers and their authorized representatives
- b) Shareholders
- c) Agents, suppliers, dealers, and merchants with whom we have agreements
- d) Prospective customers
- e) Visitors to our premises or digital platforms
- f) Users of our websites, apps, or online services
- g) Employees, contractors, and job applicants
- h) Any other persons whose data we lawfully collect in the course of our operations including beneficiaries, guarantors, next of kin, authorized signatories, directors of corporate clients, and any other person whose data is provided to us or collected by us in the course of our operations and compliance with legal or regulatory requirements. .

2. COLLECTING INFORMATION FROM YOU

We may collect and process your personal data through information that you provide us such as when you fill out application forms, through our website, face-to-face and electronic communication (including telephone conversations) in order to provide our services to you.

Our Privacy Notice does not apply when you leave our website, including third-party websites where our online advertisements are displayed or links to third-party websites which we do not operate or control. Please read the privacy statements/notices and terms and conditions of these third-party websites and decide whether they satisfactorily protect your rights.

3. THE KIND OF INFORMATION WE HOLD ABOUT YOU

We may collect, store, and use the following categories of personal data about you:

- 1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- 2. Personal information such as passport photos, Date of birth, Gender, Marital status, employment status, and Next of Kin
- 3. Financial information; estimated monthly income levels, Your credit or debit-card information, bank account numbers and or other banking information.
- 4. Copies of your identity documents such as IDs or passports
- 5. Name of your employer, terms of employment and if on contract, expiry of the contract.
- 6. Your signature specimen.

7. Your transaction information when you use our electronic and digital platforms, branches, our agents and/or merchants.
8. Your preferences for particular products and services, based on information provided by you or from your use of our network or third-party products and services.
9. Name, family details, age, profiling information such as level of education, bank account status, income brackets.
10. Your contact with us, such as when you: call us or interact with us through social media, email (we may record your conversations, social media or other interactions with us), register your biometric information such as your voice, fingerprints etc, visit our branches.
11. Information as required by Regulators, such as KYC AND AML (Know Your Client and/or Anti Money Laundering regulations) and as part of our client intake procedures. This may possibly include evidence of source of funds, at the outset of and possibly from time to time throughout our relationship with clients, which we may request and/or obtain from third party sources.

3.1. How do we obtain such information?

1. Make an application, buy or use any of our product and or service on our electronic and digital platforms.
2. When you purchase or sell shares issued by the Bank.
3. When you submit forms, update your contact or payment details, or communicate with us.
4. Use any of our product and/or service online, on a mobile or other device or in any of our branches or with any of our agents or merchants.
5. When you contact the bank with a query or a complaint or Ask for more information about a product or service;
6. Application for employment at Family Bank Limited;
7. CCTV footage and other information obtained through electronic means in our premises;
8. When you engage our insurance services or as a result of your relationship with one or more of our staff and clients;
9. When we require personal information from you in order to fulfil a statutory or contractual requirement, or where such information is necessary to enter into a contract or is otherwise an obligation, we will inform you and indicate the consequences of failing to do so;
10. When you make an application or engage with Family Foundation as a beneficiary in any of our programs.
11. We may obtain from third parties, such as information that we obtain when verifying details supplied by you and information collected from publicly available sources such as Companies Registry. Such third parties may include fraud prevention agencies, banks, merchants and credit reference agencies.
12. Other information about an individual that you or they disclose to us when communicating with us

In addition, we may collect, store and use information about you while you access our services through online means, such as the browser or device you use to access our sites and platforms, how you use the sites, traffic and location data refer to our Cookie Policy.

4 LEGAL BASIS FOR COLLECTING THE INFORMATION

This privacy notice aims to give you complete and transparent information on how we process your personal data. We are committed to ensure that your personal information is processed in a way that is compatible with the specified, explicit, and legitimate purpose of collection. We process your personal data in accordance with the Data Protection Act No. 24 of 2019

Where personal data relates to a child, we will process the personal data only where parental or legal guardian consent has been given.

We'll only use your information where we have your consent or where we have another lawful reason including:

1. To carry out our obligations from any contracts entered into between you and us or to take steps to enter into an agreement with you.
2. Verifying your identity information through publicly available and/or restricted government databases to comply with applicable Know Your Customer (KYC) requirements.
3. Assessing the purpose and nature of your business or principal activity, your financial status and the capacity in which you are entering into the business relationship with us.
4. Maintaining and administering shareholder records.
5. Processing share transactions, dividend payments, and corporate actions.
6. Facilitating communication, including notices of meetings, reports, and disclosures.
7. To meet our regulatory compliance and reporting obligations
8. To provide our services to you, manage your accounts and our relationship with you
9. To respond to your queries and complaints to us and any other requests that you may have made to us
10. Carrying out credit checks and credit scoring.
11. To keep you informed about products and services you hold with us and to send you information about products or services (including those of other companies) which may be of interest to you unless you have indicated at any time that you do not wish us to do so.
12. To prevent, detect, and investigate fraud and alleged fraud practices and other crimes
13. Any purpose related to the prevention of financial crime, including sanctions screening, monitoring of anti-money laundering and any financing of terrorist activities.
14. To verify your identity in order to protect you and your assets
15. To evaluate, develop and improve our services to you and other customers
16. To contact you, by post, phone, text, email and other digital methods. This may be for reasons such as to collect any debts owing to us.

Where processing of personal data is carried out on behalf of FBL, we have a separate contract with the processor with respect to this processing. This contract ensures compliance with Data Protection Act 2019 and defines sufficient guarantees for the implementation of appropriate technical and organizational measures, which ensure the protection of your rights

5. RETENTION OF INFORMATION

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. The statutory legal requirement is 7 years. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you. To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, the need to comply with our internal policy and the applicable legal, regulatory, tax, accounting or other requirements. Anonymized information that can no longer be associated with you may be held indefinitely.

6. DISCLOSURE AND INFORMATION SHARING

Any disclosure of your information shall be in accordance with applicable law and regulations. We shall assess and review each application for information and may decline to grant such information to the requesting party.

We may disclose your information to:

- a. law-enforcement agencies, regulatory authorities, courts or other statutory authorities in response to a demand issued with the appropriate lawful mandate and where the form and scope of the demand is compliant with the law.
- b. our subsidiaries, associates, partners, software developers or agents who are involved in delivering the bank's products and services you order or use;
- c. Fraud prevention and Anti money laundering agencies, credit- reference agencies;
- d. publicly available and/or restricted government databases to verify your identity information in order to comply with regulatory requirements;
- e. debt-collection agencies or other debt-recovery organizations;
- f. Any other person that we deem legitimately necessary to share the data with.

To help us provide services, your data will be processed internally and externally by other third parties. We use third parties for [administrative, servicing, monitoring and storage of your data]. We will outsource some services to third parties whom we consider capable of performing the required processing activities so that there is no reduction in the service standard provided to you by us.

7. YOUR RIGHTS

Subject to legal and contractual exceptions, you have rights under data protection laws in relation to your personal data. These are listed below: -

- a. Right to be informed that we are collecting personal data about you;
- b. Right to access personal data that we hold about you and request for information about how we process it;
- c. Right to request that we correct your personal data where it is inaccurate or incomplete;
- d. Right to request that we erase your personal data noting that we may continue to retain your information if obligated by the law or entitled to do so;

- e. Right to object and withdraw your consent to processing of your personal data. We may continue to process if we have a legitimate or legal reason to do so;
- f. Right to request transfer of your personal data in an electronic format.

In exercising your right as provided above, we may request specific information from you to help us confirm your identity. This is a security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

You can exercise your rights by filling these forms [Data Subject Request Forms Archives - Family Bank Limited, Kenya](#) and present at the Branch or email at dataprotection@familybank.co.ke

8. INTERNATIONAL DATA TRANSFERS

Your data is primarily stored in our data centers located within Kenya and some data resides abroad using cloud technologies and in several countries. We ensure an appropriate level of protection by the recipient of the data when we transmit your data outside Kenya, in addition, those jurisdictions must have in place Data Protection Laws.

9. MARKETING

We generally do not use your information collected on the data collection modes for marketing purposes but if you apply for products and services on the data collection modes, your information may be used to inform you about other related products and services of Family Group that may be of interest. If you do not want to receive any marketing materials, you can withdraw your consent at dataprotection@familybank.co.ke

9.1 Social Media

We operate and communicate through our designated channels, pages and accounts on some social media sites to inform, help and engage with you. We monitor and record comments and posts made about us on these channels so as to improve our services. We are not responsible for any information posted on those sites other than the information posted by our designated officials. We do not give investment, tax or other professional advice on social media sites.

As such we operate the following social channels:

- i. Facebook
- ii. Twitter
- iii. Instagram
- iv. LinkedIn

9.2 Surveys and Feedback

As with any regular survey, our online and mobile surveys are there to help gathering of specific information regarding our various services including transactional. This is in order to enhance the quality of service offering, which eventually will be reflected positively for our customers. The provision of their name and other details is totally optional however; FBL has provided an opt-out for mechanism for customer who would not like to continue participating in the surveys.

10. DATA SECURITY

We have put in place appropriate organizational and security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

11. EXCEPTIONS

We acknowledge that there will be exceptional circumstances where personal data can be processed without the data subjects' consent. There may be limitations on data subject rights when required by the law or when there are competing rights and therefore it will require an assessment based on the facts and circumstances.

12. CHANGES TO OUR PRIVACY STATEMENT

Family Bank reserves the right to amend this statement at any time. All amendments to this statement will be posted on the website.

This Privacy Statement has been updated on November, 2025.

13. THE BANK'S DATA PROTECTION OFFICER

The Bank has appointed a Data Protection Officer, whose role includes acting as a point of contact for individuals/data subjects in relation to concerns around how their data is processed. You can contact the Bank's Data Protection Officer using the details below.

Data Protection Officer

Family Bank Limited

Family Bank Towers, 6th Floor, Muindi Mbingu Street

P.O Box 74145-00200, NAIROBI.

Email: dataprotection@familybank.co.ke