

SIDIAN BANK PRIVACY NOTICE

Effective March 2023

Purpose and scope

Sidian Bank Limited is committed to protecting the privacy of personal data of all our clients and other data subjects (“**You**”).

This Privacy Notice (“**Notice**”) informs you of:

- Who we are;
- How we collect, use, store and share your personal data;
- Your privacy and other related rights under the provisions of the Data Protection Act and Regulations; and
- How to contact us or the Office of the Data Protection Commissioner (ODPC) if you have a complaint.

Please read and understand this Notice as we want to be sure that you are fully aware of how and why we are using your data.

Who are we?

Sidian Bank Limited is a commercial bank licensed and regulated by the Central Bank of Kenya. Our Head Office is at K-Rep Centre, Wood Avenue, Kilimani, P.O. Box 25363-00603, Nairobi, Kenya.

Any reference to the “**Bank**”, “**Sidian Bank**”, “**we**”, “**us**” or “**our**” includes Sidian Bancassurance Intermediary Limited, a subsidiary of Sidian Bank and any other Sidian Bank subsidiaries (including successors in title and permitted assigns).

We are the data controller for the information that we collect from you. This means that we decide how to use information about you (referred to as **personal data** – this may include your name, date of birth, address, contact information, financial information, employment details and device identifiers including IP address) and we are responsible for protecting your personal data in accordance with data protection laws and regulations.

We will outline below how we collect and use your personal data. Please note that when we refer to “processing” your personal data, we are referring to using your personal data by collecting it, using it, storing it, communicating it to other people (with your consent or as part of our service to you) or deleting it.

The terms and provisions of this Notice may be changed, updated, and amended from time to time. If we substantially or materially change the provisions of this Notice during the time

when we are providing you with our products and services, we will inform you of these changes. *Latest version

Information we hold about you

Personal data refers to any information about an individual from which that individual may be identified. It does not, therefore, include anonymised data (data where the identity has been removed).

We primarily hold information about you that we collect directly from you, for example when performing the following:

- applying for a new product or service;
- visiting our branches and premises;
- using USSD, website (sidianbank.co.ke), internet banking application, or mobile application (SidianVibe App);
- contacting us through any channels including email, telephone, or social media; or
- giving information to us at any other time.

The information we hold will include the following:

- your personal details (for example: your name, date of birth, ID number, or other identification information);
- your contact details (for example: your postal address, phone number, email address or mobile number);
- details of transactions (for example: payments you make and receive);
- financial information (for example: your bank account number, debit-card or credit-card numbers, financial history);
- property details (for example: records of personal property) if you provide these when you apply for a particular product;
- details of next-of-kin to contact the next-of-kin in the event of death or incapacity; and
- proof of income (such as payslips or bank statements) if you provide these when you apply for a particular product.

This information is needed so that we can provide products and services to you. If you do not provide the personal data asked for, we may be delayed or prevented from providing such products and services.

We may also collect information from the following:

- people appointed to act on your behalf (e.g., advisers, agents, joint account holders, lawyers);
- other banks and financial institutions;
- credit reference bureaus (who may check their information against other databases – public or private – they have access to);
- fraud prevention agencies;
- publicly available sources, such as media stories and online registers or directories;

You confirm that the individuals whose personal data you are providing to us or requesting us to share with third parties have been informed and understand how their personal data will be used by us as outlined in this Notice.

Normally we will not seek to obtain personal data from you that is referred to as sensitive personal data. Sensitive personal data includes details about your race or ethnicity, conscience, belief, sex life, sexual orientation, health, genetic data. Where we process any sensitive personal data, it is as outlined in this Notice.

Legal and lawful basis

We process your information for a variety of reasons that are necessary to provide you with the best banking experience. We primarily use your information for the following purposes:

- to provide and avail our products and services to you;
- to prevent fraud and money-laundering, and to confirm your identity before we provide services to you;
- to communicate with you;
- to protect our business interests or to prevent fraud;
- to meet obligations we have under any laws, rules, and regulations that apply to any of the products and services we provide to you; and
- 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.

Under data protection laws, we must have a lawful reason to process your personal data. In most cases, the legal basis will be one of the following:

- where you give us your consent to using your personal data (e.g., marketing communications or for conducting market research) – your consent may be

withdrawn by you at any time as set out in this Notice – withdrawal of consent does not affect the legality of data processed prior to such withdrawal.;

- for the performance of our contract with you, or to take steps at your request before entering a contract (e.g., to make and receive payments);
- to comply with our legal obligations, including anti-money laundering and counter-terrorism financing laws;
- for our legitimate interests (e.g., fraud prevention and to protect the security of our systems and services) – in this case, our interests do not outweigh your interests; and
- in the case of sensitive personal data, it is in the substantial public interest (e.g., to support you if you are or become a vulnerable customer).

The table below details the ways that we may use your personal data, the legal bases we rely on to do so, and what our legitimate interests are, where relevant.

Legal Basis	Purpose
Contractual Necessity	<ul style="list-style-type: none"> - providing products and services to you that involve opening and maintaining your account, executing transactions, administering claims where applicable, managing our risks and maintaining our overall relationship with you; - collecting and/or recovering debts, and exercising other rights we have under any agreement with you; - communicating with you and give you statements and other information about your account or our relationship with you; - providing you with further information that you request from us regarding the products or services you have with us; - compliance with specific banking product requirements (e.g., accounts, loans, securities, insurance, deposits); - handling enquiries and complaints; or - analysis of any potential needs, the provision of advice, and to support the execution of transactions.
Legitimate Interest	<ul style="list-style-type: none"> - providing and managing your accounts and our relationship with you – <i>it's in our legitimate interests to make sure that our customer accounts are well-managed to protect our business interests and the interests of our customers;</i> - handling enquiries and complaints – <i>it's in legitimate interests to make sure that complaints are investigated, resolved, and prevented from reoccurring;</i>

- conducting assessments, testing, analysis (including credit and behaviour scoring) and market research – *it’s in our legitimate interests to continually improve and innovate our operations, including the development of new systems, products, and services. This includes producing reports and statistics to enhance our offerings and maintain a competitive edge while ensuring a high level of customer satisfaction* - When conducting analysis, we may merge the information we possess with information obtained from outside sources. The resulting information we produce, and share will not identify you as an individual and cannot be attributed to you.;
- evaluating, developing, and improving our services to you – *it’s in our legitimate interest to constantly assess, enhance, or upgrade our offerings and the user experiences on our platforms to ensure high levels of service to our customers;*
- protecting our business interests and developing our business strategies – *it’s in our legitimate interest to ensure the success and growth of the Bank, by safeguarding its assets, managing its resources efficiently and effectively, and planning for its future development. This involves analysing market trends, customer needs and preferences, and other factors that could impact the business and making informed decisions about the direction of the company. By doing so, the Bank can remain competitive and provide a high level of service to its customers;*
- collecting any debts you owe to us – *it’s in our legitimate interest to ensure the efficient and effective management of our business operations, including protecting and recovering owed debts, and safeguarding our assets;*
- preventing, detecting, investigating, and prosecuting fraud and alleged fraud, money laundering and other crimes, and also checking your identity – *it’s in our legitimate interest to prevent and investigate fraud, money laundering and other crimes (including identity theft), and to check your identity in order to protect our business and comply with various laws and regulations;*
- monitor, record and analyse any communications between you and us, including phone calls – *it’s in our legitimate interest verify your instructions to us, to avoid and uncover fraud and other criminal activity (including identity theft), to analyse, evaluate, and enhance our services to customers, and for training purposes, to enhance the services we offer to our customers and to secure our business interests;*

	<ul style="list-style-type: none"> - recording your image on CCTV when you visit our premises – <i>it’s in our legitimate interest to prevent criminal activity, protect our business and comply with various laws and regulations;</i> - transferring your information to or sharing it with any organisation your account has been or may be transferred to following a restructure, sale, or takeover of any Sidian company or debt – <i>it’s in our legitimate interest to restructure or sell part of our business or any debt;</i> - sharing your information with relevant credit reference bureaus, fraud prevention agencies – <i>it’s in our legitimate interest to carry out certain credit checks so that we can make responsible business decisions. We need to make sure that we only provide certain products and services to individuals if they are appropriate and to manage the services we provide effectively, for instance, in cases where we suspect potential payment difficulties.</i> - sharing your information with relevant regulatory agencies, tax authorities, law enforcement agencies – <i>it’s in our legitimate interest help prevent and detect fraud and other crime and cooperate with lawful requests from government agencies;</i> - sharing your information with our partners and service providers – <i>it’s in our legitimate interest to use other service providers to provide some services for us or on our behalf;</i> - asserting legal claims and a defence in legal disputes – <i>it’s in our legitimate interest protect the Bank and its assets from potential legal liability and financial loss;</i> and - sending you updates about products and services you have with us, as well as information about products, services, rewards, offers, promotions, and contests (including those from other companies) that may interest you – <i>it’s in our legitimate interest to share information with you about products or services that may be relevant and beneficial to you. Where we send you marketing messages, you can always opt-out as set out in this Notice.</i>
<p>Legal and Regulatory Obligations</p>	<ul style="list-style-type: none"> - providing and managing your accounts and our relationship with you; - communicating with you and give you statements and other information about your account or our relationship with you; - handling enquiries and complaints; - providing products and services to you;

	<ul style="list-style-type: none"> - conducting assessments, testing (including system tests), and analysis (including credit and behaviour scoring); - preventing, detecting, investigating, and prosecuting fraud and alleged fraud, money laundering and other crimes, and also checking your identity; - sharing your information with relevant credit reference bureaus, fraud prevention agencies; - sharing your information with relevant regulatory agencies, tax authorities, law enforcement agencies; and - recording your image on CCTV when you visit our premises;
Consent	<ul style="list-style-type: none"> - communicating with you and give you statements and other information about your account or our relationship with you; - sending you updates about products and services you have with us, as well as information about products, services, rewards, offers, promotions, and contests (including those from other companies) that may interest you; - using your biometric data (such as fingerprint) for authentication, detecting, and preventing fraud and money laundering, and to check your identity.

Sensitive Personal Data

In accordance with data protection legislation, we may collect and process sensitive personal data, including property details, biometric data.

This data will only be used if it is deemed necessary for the purpose of:

- carrying out our obligations and exercising specific rights;
- as part of a legal proceeding; or
- if we have obtained your explicit consent.

We ensure that all legal requirements are met in the handling of this information.

Additional provisions relating to Sidian Bancassurance Intermediary Limited (SBIL)

In addition to the information set out above, SBIL may collect and process sensitive personal data outlined below.

- **Medical and health information** – including details of existing and previous physical or mental health conditions, health status, hospital admission history, test results,

medical diagnoses and treatment given, prescriptions and personal habits (e.g., smoking or use of tobacco products).

Automated decision making

Your personal data may be used in an automated decision-making or profiling process. We process some of your data automatically for;

- detecting and preventing fraud by monitoring transactions either to prevent you committing fraud, or to prevent you becoming a victim of fraud;
- carrying out automated financial crime checks such as money laundering, sanction screening, terrorism financing, and other criminal acts (including identity theft); and
- performing credit and affordability assessment checks to determine whether an application you have made will be accepted as well as to decide credit limits.

We may make automated decisions about you in the following circumstances:

- where automated decisions are necessary for us to enter a contract e.g., we may decide not to offer our services to you, or we may decide on the types of services that are suitable for you, or how much to charge you for our products, based on your credit history and other financial information we have collected about you;
- where automated decisions are required or authorised by law e.g., to prevent fraud; and
- where it is a reasonable way of implementing legal and regulatory requirements or guidance e.g., to perform financial crime checks.

We also analyse you based on your personal data, referred to as profiling, in the following circumstances:

to choose personalised offers, discounts, or recommendations to send you, based on various factors such as your credit history and how you use the accounts and products you hold with us. You can opt-out of this by using the opt-out mechanisms provided in the medium we use to contact you (e.g., email or SMS) or contacting us as provided Cookies

We employ the use of cookies and similar technologies across our websites, apps, and emails. Cookies are small text files that are stored on your computer or mobile device when you visit a website or use an app. These cookies are then recognized by the website or app upon subsequent visits.

We use cookies to do many different jobs, such as gathering information to improve your online experience by remembering your preferences, and letting you efficiently navigate between pages.

Our cookie policy on our websites and apps provides additional information about cookies, how and where we use them, and how you can control them.

- Complaints section below.

You have rights relating to automated decision-making. If you want to know more, please contact us using the details set out in the Cookies

We employ the use of cookies and similar technologies across our websites, apps, and emails. Cookies are small text files that are stored on your computer or mobile device when you visit a website or use an app. These cookies are then recognized by the website or app upon subsequent visits.

We use cookies to do many different jobs, such as gathering information to improve your online experience by remembering your preferences, and letting you efficiently navigate between pages.

Our cookie policy on our websites and apps provides additional information about cookies, how and where we use them, and how you can control them.

Complaints section below.

Sharing your information

We will keep your information confidential, but we may share it with third parties (who are also legally and/or contractually mandated to keep it secure and confidential) in the following circumstances:

Third Party	Purpose
Sidian subsidiaries, Bank agents, and Branch network	We may share certain information with other Sidian companies (for example, to provide you with products or services, for marketing purposes, for internal reporting and where those companies provide services to us) and our Bank Agents and Branch Network to enable us to provide a service you have requested.
Other credit and financial services institutions or similar institutions	We may share personal data within the context of their business relationship with you (e.g., correspondent banks, custodian banks, brokers, insurance, and information agencies)
Government agencies (e.g., CBK, KRA, FRC, IRA and law enforcement agencies)	We may share personal data with government and regulatory agencies in connection with their lawful duties (such as preventing and investigating crime)
Credit reference bureaus (CRBs)	We may share personal data with CRBs to carry out credit and identity checks on you. During the time you are our customer, we will exchange information about you and your accounts with the CRBs. They may then share your personal information with other organizations who may use it to make decisions about you – this may

	impact your ability to obtain credit. Even after your account is closed, we may still gather information about you from the CRBs.
Fraud prevention agencies and other similar third parties	We may share personal data in connection with actual or suspected fraud, financial crime, or criminal activities, or with monitoring, preventing, and investigating fraud, financial crime, or criminal activities.
Providers of payment-processing services	We may share personal data with payment-processing companies and other businesses that assist us in processing your payments, as well as financial institutions that are members of the payment schemes (e.g., Visa) or involved in making payments for specific types of payment.
Our service providers and agents (including their subcontractors)	We may share personal data with our service providers, this may include, for example, third-party collection agents we use, or where we pass your details to someone who will print your statements or deliver a debit/credit cards/cheque book. We may also ask third-party providers who act on your behalf to share your information with our agents or sub-contractors to enable us to provide a service you have requested.
Business partners	We may share personal data with our partner companies with whom we offer services with, such as credit or debit card issuers (or those whose name or logo appears on a credit card or debit card we provide to you). This may also include sharing information with third-party service providers or agents who act on behalf of our business partners.
Your advisers	We may share personal data with your advisers (such as accountants, lawyers, and other professional advisers) who you have authorised to represent you, or any other person you have told us is authorised to give instructions, or use the account, products, or services, on your behalf (such as under a power of attorney)
Independent third-party service providers	We may share your personal data with third-party service providers that you, or an authorized third-party, request us to share information with, such as providers of payment-initiation or account-information services. If we do share your information with these third parties, we will no longer have control over its usage.
Any third party after a restructure, sale, or acquisition	We may share personal data with a third party after a restructure, sale, or acquisition of any Sidian company or debt, as long as the third party uses your information for the same purposes you originally gave it us for.
Insurance providers	We may share personal data with insurance providers including underwriters, brokers, introducers, claims handlers and other such associated third parties to enable us to provide a service you have requested.

Third party payers	We may share your name with anyone paying money into your account if this is necessary to confirm the payment is being made to the right account.
---------------------------	---

Storing and retaining your information

We will ordinarily retain your information for a minimum period of seven (7) years to enable Sidian to comply with regulatory and contractual requirements unless there is a particular reason to hold records for longer, including legal hold – a process that the Bank uses to preserve all forms of relevant information when litigation is reasonably anticipated which require us to keep records for an undefined period of time.

The length of time we retain your data will also depend on the nature of the data and the purposes for which it was collected. When it is no longer necessary to retain your personal data, we will securely delete or anonymize it.

We have implemented security measures to protect your personal data from being lost, misused, or accessed without permission. Only individuals with a valid need to access the data will be granted access, and appropriate measures will be taken to maintain confidentiality during processing.

Transferring your data out of the Republic of Kenya

Your information may be transferred to and stored in locations outside of Kenya. When we do this, we will make sure that:

- organisations we transfer your information to apply an equivalent level of protection to your information as we do; and
- we include conditions in the contract with the organisations receiving your personal information to protect it to the standard required in the Data Protection Act and Regulations.

These transfers may be necessary to:

- fulfil our contractual obligations to you,
- meet legal obligations,
- protect the public interest, or
- for the sake of our legitimate interests.

Your legal rights

You have several rights in relation to your personal data. These include the right to:

- ask for a copy of personal data we hold about you (Right of access);

- ask us to give you (or a third party chosen by you) an electronic copy of the personal data you have given us (Right to data portability);
- ask us to correct personal data we hold (Right to rectification);
- restrict how we use your personal data (Right to restriction of processing);
- ask us to delete personal data (Right of erasure);
- object to particular ways we are using your personal data (Right to object);
- object to any automated decision-making; and
- withdraw any permission you have previously given to allow us to use your information.

Your ability to exercise these rights may be influenced by several factors. In some cases, we may not be able to accede to your request due to a valid reason or if the specific right is not applicable to the information we possess concerning you.

Cookies

We employ the use of cookies and similar technologies across our websites, apps, and emails. Cookies are small text files that are stored on your computer or mobile device when you visit a website or use an app. These cookies are then recognized by the website or app upon subsequent visits.

We use cookies to do many different jobs, such as gathering information to improve your online experience by remembering your preferences, and letting you efficiently navigate between pages.

Our cookie policy on our websites and apps provides additional information about cookies, how and where we use them, and how you can control them.

Complaints

Should you have any complaints or queries about anything relating to the privacy of your personal data, or any other data protection issues, please let us know through:

Address: Sidian Bank Limited, K-Rep Centre, Wood Avenue, Kilimani, P.O. Box 25363-00603, Nairobi, Kenya | [+254 711 058 994](tel:+254711058994)

Email: **Sidian Bank Limited:** dpo@sidianbank.co.ke

Sidian Bancassurance Intermediary Limited: dpoassurance@sidianbank.co.ke

However, you also have the right to make a complaint at any time to the ODPC, which is the supervisory authority for data protection issues in the Republic of Kenya. You may lodge a complaint with the ODPC through: <https://www.odpc.go.ke/file-a-complaint/>.