izola Bank

PRIVACY POLICY

1. Introduction

The Bank is committed to safeguard your privacy at all times.

This Privacy Policy applies where the Bank acts as a data controller in respect of personal data, meaning that the Bank determines the purposes and means of processing that personal data.

In this policy, 'the Bank' refers to 'Izola Bank plc'.

Izola Bank plc is licensed as a credit institution in terms of the Banking Act (Cap. 371 of the Laws of Malta).

2. Amendments

The Bank may update this Privacy Policy from time to time by publishing an updated version on its websites. The date of the latest update will be indicated in this Privacy Policy. Where appropriate, the Bank may notify you of material changes by email or through another suitable communication method.

3. The controller's details

The Bank (Izola bank plc, the data controller) is registered in Malta under registration number C-16343, and the registered office is at 4, Castille Place, Valletta VLT1062 Malta.

You can contact the Bank by visiting the Help centre.

4. How the Bank uses your personal data

The general categories of personal data that the Bank may process include:

- Personal details such as your name, identification number, date of birth, KYC (Know Your Client) documents including a copy of your national identity card or passport, phone number, physical and electronic address, and family details such as the name of your spouse, partner, or children;
- Financial information, including payment and transaction records and information relating to your assets (including fixed properties), financial statements, liabilities, taxes, revenues, earnings and investments (including your investment objectives);
- Tax domicile and other tax-related documents and information;
- Professional information about you, such as your job title and work experience;
- Details of the Bank's interactions with you and the Bank's products and services you use;
- Any records of phone calls between you and Izola Bank;

- Identifiers that the Bank will assign to you, such as your client or account number;
- Data transmitted by your browser when you access the Bank's websites which is automatically recorded by the Bank's server, including date and time of the access, name of the accessed file as well as the transmitted data volume and the performance of the access, your web browser, browser language and requesting domain, and IP; and
- Information from public registers which, depending on the product or service, may include beneficial ownership and other registers, public administration or other third-party sources, such as wealth screening services, credit reference agencies, fraud prevention agencies and intermediaries that facilitate data portability.
- Information relating to your use of the Bank's Digital Banking Services, including your username, name and surname, phone number and email address;
- Technical information about your use of the Bank's Digital Banking Services, including device information, IP address, browser type and version, operating system, login times, pages visited, time spent on pages and unique device identifiers;
- User preferences and settings related to your Digital Banking Services, including authentication preferences, language settings, notification preferences, and other customizable features;
- In the case of BOE (Bills of Exchange), the Bank collects and processes your personal data through its third-party clients. The categories of personal data collected are required for the Bank to provide client funding and comply with other regulations.
- In the case of home loans, the Bank may collect and process your personal data through credit intermediaries. The categories of personal data collected are required for the Bank to make a credit decision, provide the service and comply with the related regulations, including but not limited to Malta Central Bank's Directive Number 16 and Anti-Money Laundering laws and regulations.

Sources of personal data

The Bank may obtain personal data directly from the individual concerned or from other sources, including:

- public registers and public authorities;
- credit intermediaries;
- corporate clients, counterparties and other persons involved in a transaction;
- credit-reference and fraud-prevention agencies;
- sanctions, screening and identity-verification providers;
- payment participants, correspondent institutions and other financial institutions;
- service providers and business partners; and
- other sources where obtaining the information is permitted or required by law.

Personal data obtained from these sources may include identification, contact, professional, financial, transactional, beneficial-ownership, credit, fraud-prevention and regulatory-compliance information.

Legal basis for processing

The Bank processes personal data only for specified purposes and limits the personal data processed to what is relevant and necessary for those purposes. In particular, the Bank processes personal data to:

- necessary for the legitimate interests of the Bank, without unduly affecting your interests or fundamental rights and freedoms
- necessary for taking steps to enter into or executing a contract with you for the services or products you request, or for carrying out the Bank's obligations under such a contract;
- required to meet the Bank's legal or regulatory responsibilities;
- in some cases, necessary for the performance of a task carried out in the public interest;
- in limited circumstances, processed with your consent which the Bank obtains from you from time to time.

Legitimate interests

Where the Bank relies on legitimate interests, those interests may include:

- protecting customers, employees, systems and services;
- preventing and detecting fraud and other unlawful activity;
- administering and improving products, services and systems;
- managing customer and business relationships;
- recovering debts;
- exercising and protecting the Bank's legal rights; and
- ensuring the effective and secure operation of the Bank's business.

Before relying on legitimate interests, the Bank considers whether those interests are compatible with the rights and freedoms of the individuals concerned.

Requirement to provide personal data

Certain personal data is required by law or is necessary for the Bank to enter into or perform a contract with you. If the required information is not provided, the Bank may be unable to assess an application, open or maintain an account, provide a requested product or service, execute a transaction, or comply with its legal and regulatory obligations. Where providing personal data is optional, this will be indicated at the relevant point of collection.

Purposes of processing

The Bank always processes your personal data for a specific purpose and only processes the personal data which is relevant to achieve that purpose. In particular, the Bank processes personal data to:

- conduct your onboarding processes, including to verify your identity and assess your application if you apply for credit, and to conduct legal and other regulatory compliance checks (for example, to comply with anti-money laundering regulations and to prevent fraud);

- provide products and services to you and ensure their proper execution, for instance by ensuring that the Bank can identify you and make payments to and from your accounts in accordance with your instructions and the product terms;

- manage the relationship with you, including communicating with you in relation to the products and services you obtain from the Bank and from its business partners, handling customer service related queries and complaints, facilitating debt recovery activities, making decisions regarding credit or your identity, and closing your account (in accordance with applicable law) if it remains dormant and the Bank is unable to contact you after a period of time;

- help the Bank to learn more about you as a customer, the products and services you receive, and other products and services you may be interested in receiving, including profiling based on the processing of your personal data, for instance by looking at the types of products and services that you use from the Bank, how you like to be contacted and so on;

- take steps to improve the Bank's products and services and the Bank's use of technology, including testing and upgrading of systems and processes, and conduct market research to understand how to improve the Bank's existing products and services or to learn about other products and services the Bank can provide;

- contact you for direct marketing purposes about products and services the Bank thinks will be of interest to you and facilitate competitions and promotions;

- meet the Bank's ongoing regulatory and compliance obligations (e.g. laws of the financial sector, anti-money-laundering and tax laws). These may include:

- the recording and monitoring of communications;

  - disclosures to tax authorities, financial service regulators and other regulatory and governmental bodies, and;
  - investigating or preventing crime.

- ensure the safety of the Bank's customers, employees and other stakeholders;

- undertake transactional and statistical analysis, and related research;

- process underwriting.

- provide and maintain the Bank's Digital Banking Services, secure authentication processes, and facilitate the functionalities of the Internet Banking Service and Mobile Banking App;

- enable you to view account balances, transaction history, make payments and transfers, and perform other banking operations through the Bank's Digital Banking Services

Personal data will not be used for any decision solely taken on the basis of automated decision-making processes, including profiling, without human intervention. Prior to the provision of the Bank's services, the Bank may collect information from you in order to, amongst others, comply with the Bank's obligations at law, determine your risk profile and/or for any other purpose connected with the agreement of service. The Bank may process your personal data on the basis of and/or pursuant to the performance of such agreement and/or the performance of the Bank's obligations at law. As stated, no automated decision will result from the Bank's use of such systems.

Depending on the circumstances, the Bank relies on the following lawful bases:

- Onboarding, identity verification and application assessment: steps necessary to enter into a contract and compliance with legal and regulatory obligations;

- Providing and administering banking products and services: performance of a contract and compliance with legal obligations;

- AML, sanctions, tax, fraud-prevention and regulatory reporting: compliance with legal obligations and, where applicable, performance of a task in the public interest;

- Security and fraud prevention: compliance with legal obligations and the Bank's legitimate interests in protecting individuals, systems and services;

- Handling enquiries, complaints and debt recovery: performance of a contract, compliance with legal obligations and the Bank's legitimate interests in administering relationships and protecting legal rights;

- Service improvement, research and statistical analysis: the Bank's legitimate interests in evaluating and improving products, services, systems and customer journeys; and

- Direct marketing: consent or legitimate interests, as applicable, subject to applicable electronic-marketing requirements.

Providing your personal data to others

The Bank may disclose your personal data to any member of the Bank's group of companies, which means the Bank's ultimate holding company and all its subsidiaries, insofar as reasonably necessary for the purposes as set out in this n.

In respect of home loan services, personal data may be exchanged between the Bank and its authorised credit intermediaries.

The Bank may also disclose personal data to third parties where lawful and necessary for the purposes described in this Privacy Policy. Such third parties may be:

- a party acquiring interest in, or assuming risk in or in connection with, the transaction (such as an insurer);
- payment recipients, beneficiaries, account nominees, intermediaries, and correspondent and agent banks;
- clearing houses, and clearing or settlement systems; and specialized payment companies or institutions such as SWIFT;
- central banks and other regulatory bodies such as MFSA;
- system suppliers, service providers and other outsourced data processors;
- market counterparties;
- stock exchanges
- other financial institutions, credit reference agencies or credit bureau (for the purposes of obtaining or providing credit references)
- parties interested in a potential and/or actual transfer of business or assets for the purpose of assessing such business or assets and/or performing any obligations assumed from the Bank as part of such transfer of business or assets.

International transfers of your personal data

In this section, the Bank will provide information about the circumstances in which your personal data may be transferred to countries outside the European Economic Area ("EEA"). Your personal data may be transferred to other controllers or processors, and/or stored in locations outside the European Economic Area (EEA), including countries that may not have the same level of protection for personal information. When the Bank does this, it will ensure that the transferee has an appropriate level of protection and that the transfer is lawful. The Bank may need to transfer your information in this way to carry out the Bank's contract with you, to fulfil a legal obligation, to protect the public interest and/or for the Bank's legitimate interests e.g. for tax authorities or anti-money laundering.

Where required, the Bank implements appropriate safeguards for transfers of personal data outside the EEA in accordance with applicable data protection law. These safeguards may include an adequacy decision of the European Commission, the European Commission's Standard Contractual Clauses, together with supplementary measures where necessary, or another lawful transfer mechanism available under applicable data protection law.

Even in these cases, the Bank will only share your information with people who have the right to see it.

You can obtain more details of the protection given to your information when it is transferred outside the EEA by contacting the Bank using the details provided in the controller's details section.

Retaining and deleting personal data

This section sets out the Bank's data retention policies and procedure, which are designed to help ensure that it complies with the legal obligations in relation to the retention and deletion of your personal data.

Your personal data that the Bank processes for any purpose shall not be kept for longer than is necessary for that purpose, unless other overriding regulations oblige the Bank to hold such data for longer.

As a general overview and also as set out in the GDPR banking industry guidelines, the Bank's retention notice for banking operations is as follows:

Archival material	Retention periods
Documentation to be kept in terms of Article 163 of the Companies Act/ Article 19 of the Income Tax Management Act.	10 years, starting from the end of the relative financial year.
Transaction Data	10 years from the date of the transaction.
Account Data	10 years from the date of closure of the account.
Telephone Recordings	10 years from the date of recording, if this is the only proof of a debit authority or of a contract. Otherwise, maximum 30 days, but if recordings are used for training purposes, retention period is at bank's discretion, provided recordings are suitably edited.
Video Recordings	Maximum 30 days for customer-facing footage (unless footage is required in connection with an ongoing investigation). Maximum 90 days for back-office operations footage.
Staff Records: Periodically reviewed records (e.g. attendance, vacation leave, sick leave) Records kept for the entire duration of the employment relationship: Payroll and other financial records Other employment records	1 year is deemed sufficient, unless specific disputes arise. 10 years following termination of employment. Maximum 5 years following termination of employment.
Internal Documentation	At Bank's discretion, provided no personal data which is not public is contained therein.
Deceased Customers' Files	10 years from when the account balance was fully distributed to the heirs.
Transaction Information	6 years from the date of the transaction.
Account Information	6 years from the date when the account was closed
Obsolete Collateral (Security) Item	6 years from the date when the item was discharged
Advances Files (Including "Classified Debt" files)	6 years from the date when the facility was closed (unless legal proceedings are in train). Note: "Old" advances files, other than files relating to home loans, need not be retained for more than 30 years, even if facilities to the customer concerned was ongoing.

Archival material	Retention periods
Investment Services: Fact finds, KYC records or similar investment- related reviews, portfolio management instructions, statements of compliance, etc. Other documentation related to the sale of investment products	6 years after the end of the investment relationship. 6 years from the date when the sale was concluded.
Documentation related to Home Loan products	To be retained for the duration of the service plus a period of six years thereafter.
Documentation related to all other contracts (e.g. safe deposit lockers, guarantees issued by the banks, letters of credit, etc.)	6 years from the date when the contract is terminated, paid off or expired.
Digital Banking Services refers to the Bank's Internet Banking and Mobile App.	10 years from the date when the account was closed.

Where the Bank process your personal data and that processing is based solely on consent, your personal data shall be deleted upon your withdrawal of such consent, or, at the point where the purpose for holding your personal data is no longer valid.

The Bank's Digital Banking Services may utilise technologies such as cookies and session-based methods to collect information about your use of the Service. This could help improve performance, user experience, and security. Depending on the version of the Bank's Digital Banking Services and your device, some of these technologies may be managed or controlled through your device settings. Some data, such as essential session-based information which is required for the Services to operate, may not be altered or deleted.

5. Website and Digital Banking session data

When the website or Digital Banking Services are accessed, the Bank may process technical and session information, including IP address, device and browser information, login and session identifiers, access times, pages or functions used, and security-related information. This information is processed to provide and secure the relevant service, prevent fraud, maintain session continuity, diagnose technical issues and protect the Bank's systems and users. The applicable lawful basis depends on the relevant service and may include performance of a contract, compliance with legal obligations and the Bank's legitimate interests in maintaining secure systems and services.

6. Keeping your data secure

The Bank shall implement and maintain appropriate and sufficient technical and organizational security measures, taking into account the nature, scope, context and purposes of the processing, to protect your personal data against any unauthorized accidental or unlawful destruction or loss, damage, alteration, disclosure or access to personal data transmitted, stored or otherwise processed and shall be solely responsible to implement such measures.

Security for Digital Banking Services

The Bank implements appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. The measures applied take into account the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of individuals.

For your own protection, please ensure that you:

- Keep your login credentials confidential and do not share them with third parties;
- Report any unauthorized activity on your account immediately by contacting the Bank through the Help centre;
- Keep the device that you use to access the Bank's Digital Banking Services secure and use the latest version of the Internet Banking Service and the Mobile Banking App;
- Do not install or use the Digital Banking Services on a jail-broken or rooted device as these have had their security features altered and are less secure;
- Ensure that you close the Internet Banking Service webpage and/or the Mobile Banking App when they are not in use.

The Bank shall ensure that the staff who process your data are aware of such technical and organizational security measures and the Bank shall ensure that such staff are bound by a duty to keep your personal data confidential.

The technical and organizational security measures in this clause shall mean the particular security measures intended to protect your personal data in accordance with any privacy and data protection laws.

7. Where you provide the Bank with personal data related to third-party data subjects

If you are a trader, a company, an intermediary or other corporate entity, and you supply the Bank with personal data of third-party data subjects such as your employees, affiliates, service providers, customers or any other individuals connected to your business, you shall be solely responsible to ensure that:

- you immediately bring this Privacy Notice to the attention of such data subjects and direct them to it;
- the collection, transfer, provision and any processing of such personal data by you fully complies with any applicable laws;
- as data controller you remain fully liable towards such data subjects and shall adhere to all applicable laws;
- you collect any information notices, approvals, consents or other requirements that may be required from such data subjects before providing the Bank with their personal data;
- you remain responsible for making sure the information you give the Bank is accurate and up to date, and you must tell the Bank if anything changes as soon as possible.

You hereby fully indemnify the Bank and shall render the Bank completely harmless against all costs, damages or liability of whatsoever nature resulting from any claims or litigation (instituted or threatened) against the Bank as a result of your provision of said personal data to the Bank.

8. Your rights as a data subject

In this section, the Bank has summarized the rights that you have under the EU General Data Protection Regulation (EU) 2016/679 ("GDPR"). Due to the complexities of some of the rights, not all of the details found at law were included in this policy with respect to your rights. Should you require any clarification please contact the Bank's DPO (Data Protection Officer). The Bank also refers you to the relevant privacy laws and guidance from the regulatory authorities for a full explanation of these rights, including but not limited to the GDPR and the Data Protection Act, Chapter 586 of the Laws of Malta, as may be amended from time to time (the "Applicable Privacy Laws").

Subject to the conditions and limitations established by applicable data protection law, you have the following rights in relation to your personal data:

- Right of Access – You have the right to ask whether the Bank processes your personal data. If the Bank processes your personal data, you may request access to that data and obtain a copy, together with the information required under applicable data protection law.

- You can also access your personal data through the facility that is made available on the online portal, or, if such facility is not available, by sending an email directly to the Bank's Data Protection Officer (the "DPO"). The details of the Bank's designated DPO are in the last section of this policy.

- You have the right to rectify any inaccurate personal data about you and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

- Some of the categories of personal data can be updated by the data subject through the facility that is made available on the online portal, or, if such facility is not available, by sending an email directly to the Bank's DPO (Data Protection Officer). The details of the Bank's designated DPO are found in the last section of this policy
- Right to Complain – you have the right to lodge a complaint regarding the processing of your personal data with the supervisory authority for data protection matters.

- In Malta this is the Information and Data Protection Commissioner at: https://register.idpc.org.mt/report-breach/complaint/

- Right to Erasure – in certain circumstances you may request that the Bank deletes the personal data that the Bank holds about you.

- Right to Object – you have a right to object and request that the Bank stops the processing of your personal data where the Bank relies on it or a third party's legitimate interest for processing your personal data.

- Right to Portability – you may request that the Bank provides you with certain personal data which you have provided in a structured, commonly used and machine-readable format. Where technically feasible, you may also request that the Bank transmits such personal data to a third party controller indicated by you.

- Right to Rectification – you have the right to update or correct any inaccurate personal data which the Bank holds about you.

- Right to Restriction – you have the right to request that the Bank stops using your personal data in certain circumstances, including if you believe that the Bank is unlawfully processing your personal data or/and the personal data that the Bank holds about you is inaccurate.

- Right to Withdraw your Consent – you have a right to withdraw consent at any time. Where the Bank's processing is based only on your consent, withdrawal of your consent shall not affect the lawfulness of any processing carried out prior to the withdrawal of your consent and

- Right to be Informed of the Source – where the personal data the Bank holds about you was not provided to the Bank directly by you, you may also have the right to be informed of the source from which your personal data originates.

Please note that your rights in relation to your personal data are not absolute and the Bank may not be able to entertain such a request; for instance, if the Bank is prevented from doing so in terms of a statutory obligation imposed on the Bank by law.

You may exercise any of your rights in relation to your personal data, where applicable, through the online portal facility, or, if such facility is not applicable or available, by sending an email directly to the Bank's DPO (Data Protection Officer). The details of the Bank's designated DPO are given below.

9. Data Protection Officer

The Bank's data protection officer will be available to respond to any data protection related requests and queries you may have. If you wish to contact the DPO, please do so by sending an email to dpo@izolabank.com.

Last updated: 05/10/2026

Issued by Izola Bank plc, Company Registration No. 16343 having its registered address at 4, Castille Place, Valletta VLT1062, Malta.
Izola Bank p.l.c. is licensed to undertake the business of banking in terms of the Banking Act (CAP 371 of the Laws of Malta) and is regulated by the MFSA (Malta Financial Services Authority).