izola Bank

PRIVACY POLICY

1. Introduction

We at Izola Bank are committed to safeguard your privacy at all times.

This policy applies where we are acting as a data controller with respect to your personal data; in other words, where we determine the purposes for and means of processing of your personal data.

In this policy, “we”, “us” and “our” refer to “the Bank, Izola Bank”.

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

2. Amendments

We may update this policy from time to time by publishing a new version on our websites. You should check this page occasionally to ensure that you are happy with any changes to this policy.

We may notify you of changes to this policy by email or other means.

3. The controller’s details

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

You can contact us by visiting our Help Centre;

4. How we use your personal data

The general categories of personal data that we may process

General categories of personal data that we 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 our interactions with you and the Bank’s products and services you use;
- Any records of phone calls between you and Izola Bank;
- Identifiers we assign to you, such as your client or account number;

- Data transmitted by your browser when you access our websites which is automatically recorded by our 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 our Digital Banking Services, including your username, name and surname, phone number and email address;
- Technical information about your use of our 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.

Legal basis for processing

Depending on the purpose of our processing activity, the processing of your personal data is:

- 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 our obligations under such a contract;
- required to meet our 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 we obtain from you from time to time.

Purposes of processing

We always process your personal data for a specific purpose and only process the personal data which is relevant to achieve that purpose. In particular, we process 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 we can identify you and make payments to and from your accounts in accordance with your instructions and the product terms;
- manage our relationship with you, including communicating with you in relation to the products and services you obtain from us and from our 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 we are unable to contact you after a period of time;
- help us 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 us, how you like to be contacted and so on;
- take steps to improve our products and services and our use of technology, including testing and upgrading of systems and processes, and conduct market research to understand how to improve our existing products and services or to learn about other products and services we can provide;
- contact you for direct marketing purposes about products and services we think will be of interest to you and facilitate competitions and promotions;
- meet our 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 our customers, employees and other stakeholders;
- undertake transactional and statistical analysis, and related research;

- process underwriting;
- provide and maintain our 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 our 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, we may collect information from you in order to, amongst others, comply with our obligations at law, determine your risk profile and/or for any other purpose connected with the agreement of service. We may process your personal data on the basis of and/or pursuant to the performance of such agreement and/or the performance of our obligations at law. As stated, no automated decision will result from our use of such systems.

Providing your personal data to others

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

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

We may also disclose your personal data to third parties where lawful to do so. 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, we 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 we do this, we'll ensure that the transferee has an appropriate level of protection and that the transfer is lawful. We may need to transfer your information in this way to carry out our contract with you, to fulfil a legal obligation, to protect the public interest and/or for our legitimate interests e.g. for tax authorities or anti-money laundering.

We have ensured the lawful processing of your personal data by putting in place the appropriate safeguards in accordance with the applicable privacy laws. With our data processors we have included EU Model Clauses in their service agreements or/and considered the applicability of the Privacy Shield protection for US based processors.

Even in these cases, we 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 us using the details provided in the controller's details section.

Retaining and deleting personal data

This section sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of your personal data.

Your personal data that we process 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 issued by the Malta Banking Association (MBA), the Bank's retention policy 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 date of transaction.
Account Information	6 years from the date when the account is 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 has been 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 have been 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 we 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.

Our 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 Our 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. Session Data

We may use session data to enhance your experience, maintain security, and ensure the proper functioning of our services.

6. Cookies that we may use

We may ask you to consent to the use of cookies in accordance with the terms of this policy when you first visit our website or use our Digital Banking Services.

Website Cookies:

Strictly necessary cookies

These cookies enable the user to have the best possible service when browsing our website.

Performance and tracking cookies

Performance and tracking cookies are used to further improve our websites. These cookies collect information about how the websites are being used (example which pages are mostly visited). All information gathered is anonymous and no personal data is obtained which might identify you as an individual. These cookies may include the following:

- Which websites are visited most often
- How long the users spend time on the websites

Functionality cookies

These cookies are used to memorize options that you choose (such as language or the region) when using our website. The information these cookies collect is anonymous and they cannot track your browsing activity on other websites. These cookies may enhance the overall experience that the client has on the websites.

Session cookies

These expire when you close the browser, due to lack of activity or at logging off from our website.

Why we use cookies

Below is a list of why we use cookies.

- You may see a pop-up welcome message when you first visit our websites.
- We will store a cookie so that your computer memorizes that the webpage or Digital Banking Service was previously visited, and such pop-ups would not show up again on your subsequent visits.
- We collect a session ID to anonymously identify your browsing session.
- We may store your details securely to facilitate your login process.
- Our online application forms require the cookies to be enabled, so we would be able to improve our understanding of how the users navigate our websites.
- To improve our understanding of how you navigate through our websites so we can identify improvements.
- To temporarily store input information in our calculators, tools, illustrations and demonstrations.
- To provide you with adverts that are more relevant to your interests, improve our targeting and enhance your journey through our websites and partner websites.
- To ensure your security and your privacy when browsing our secure websites or online banking.
- To evaluate our sites' advertising and promotional effectiveness (we own the anonymous data collected and don't share it with anyone); and we use both our own (first-party) and partner companies' (third-party) cookies to support these activities.
- To find out which pages are most relevant to you.

Cookies that we do not use

We do not use cookies that:

- Keep details that can personally identify you.
- Track your browsing after you left our websites.
- Sell or distribute information about you without your consent.

Cookies used by our service providers

We use Google Analytics to analyze the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google's privacy policy is available at: https://www.google.com/policies/privacy/.

Disable cookies

To ensure that we can provide suitable content that meets your needs, cookies should be enabled. You may not be able to utilize our Digital Banking Services, including the online internet banking and Mobile Banking App, if you opt out of all cookies from the portal.

You may disable cookies through your internet browser. Find out more by either accessing www.allaboutcookies.org/manage-cookies/ or by sending us an email on dpo@izolabank.com.

More information about cookies

For more information about cookies please refer to www.allaboutcookies.org.

7. Keeping your data secure

We 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

We take the security of our Digital Banking Services very seriously. When accessing our Digital Banking Services, we use industry-standard security measures to protect your personal data. Please ensure that you read our Security page before accessing the Digital Banking Services and follow the security recommendations provided there. You should ensure that any device you use to access our Digital Banking Services is free from and adequately protected against computer viruses and malware.

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 us through our help centre;
- Keep the device that you use to access our 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.

We shall ensure that our staff who process your data are aware of such technical and organizational security measures and we 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.

Where you provide us 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 us 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 Policy 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 us with their personal data;
- you remain responsible for making sure the information you give us is accurate and up to date, and you must tell us if anything changes as soon as possible.

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

Your rights as a data subject

In this section, we have 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 have been included in this policy with respect to your rights. Should you require any clarification please contact our DPO (Data Protection Officer). We also refer 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 440 of the Laws of Malta, as may be amended from time to time (the “Applicable Privacy Laws”).

For as long as we retain your personal data, you have certain rights under the applicable privacy laws, including:

- Right of Access – You have the right to obtain from us confirmation as to whether or not we process your personal data and, where we do, access to your personal data. The Bank shall provide the first electronic or hardbound copy of your personal data free of charge, but additional copies may be subject to a justifiable fee.
- 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 we delete the personal data that we hold about you.
- Right to Object – you have a right to object and request that we stop the processing of your personal data where we rely on our or a third party's legitimate interest for processing your personal data.
- Right to Portability – you may request that we provide you with certain personal data which you have provided to us in a structured, commonly used and machine-readable format. Where technically feasible, you may also request that we transmit 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 we hold about you.
- Right to Restriction – you have the right to request that we stop using your personal data in certain circumstances, including if you believe that we are unlawfully processing your personal data or/and the personal data that we hold about you is inaccurate.
- Right to Withdraw your Consent – you have a right to withdraw consent at any time. Where our 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 we hold about you was not provided to us 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 we may not be able to entertain such a request; for instance, if we are prevented from doing so in terms of a statutory obligation imposed on us 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.

8. Data protection officer

Our 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.