Privacy Notice

August 2023

justbank

Contents

1. WHO WE ARE

1.1. We are IDT Financial Services Limited trading as justbank ("**the bank**", "**we**" or "**us**").
1.2. We are regulated and authorised by the Financial Services Commission, Gibraltar.
1.3. We are committed to protecting the privacy of your data and this notice provides you with the necessary information regarding your privacy rights and our obligations, and explains how, why, and when we process your data when you visit and use our website and when you open an account with us.
1.4. We are a **data controller** in respect of personal information that we process in connection with our business (including the products and services that we provide) and we are subject to the Gibraltar GDPR and Data Protection Act 2004.
1.5. We respect individuals' rights to privacy and to the protection of personal information.
1.6. This Privacy Notice should be read in conjunction with our Terms & Conditions and any other privacy notices we may provide from time to time.
1.7. We have a separate Cookie Policy specific to the use of our website.
1.8. Throughout our website we may link to other websites owned and operated by certain trusted third parties (e.g., for verification purposes and to conclude payments on your behalf). Those third-party websites may also gather information about you in accordance with their own separate privacy policies. For privacy information relating to those third-party websites, please consult their privacy policies as appropriate.

2. TERMINOLOGY

The following is a list of common terms used throughout this Privacy Notice and a brief explanation of their meaning:

Term	Definition
Personal Information/Data	Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Information/Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.
Data Subject	A living identified or identifiable individual about whom we hold Personal Data. In other words, a Data Subject is an end user whose personal data can be collected.
Data Controller	Any organization, person, or body that determines the purposes and means of processing personal data, controls the data and is responsible for it, alone or jointly with others.
EU GDPR	The General Data Protection Regulation (GDPR) was adopted as Regulation (EU) 2016/679 of the European Parliament and of the Council on April 27, 2016. Its main objective is to harmonise and standardise Data Protection legislation and standards across European states.
Gibraltar GDPR	Gibraltar's' own interpretation of the EU GDPR and transposed to local law on 1st January 2021. It offers privacy protections and guarantees in a similar manner. The legislation has been amended to reflect Gibraltar's departure from the EU under BREXIT.
Data Protection Act 2004	Gibraltar specific data protection legislation, which dovetails with the Gibraltar GDPR to provide Gibraltar specific derogations and exemptions. The legislation has been amended to reflect Gibraltar's departure from the EU under BREXIT.
Data Processor	A data processor processes the data on behalf of the data controller. Examples include payroll companies, accountants, and market research companies.
Data Processing	any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction
EEA	Stands for the **European Economic Area** – includes all the countries of the European Union, plus Iceland, Liechtenstein, and Norway. From 31 January 2020The United Kingdom and Gibraltar are not part of the EEA.

3. THE INFORMATION WE PROCESS

3.1. We collect and process various categories of Personal Information at various stages of our relationship, but primarily at the start of it. We will limit the collection and processing of information to only what is necessary to achieve one or more legitimate purposes as identified in this notice.

3.2. The types of Personal Information we collect are listed below depending on the type of services we provide. In some instances, we may require these details to be independently verified by an approved verifier.

Information	Examples
Basic Personal Information/Data	• Name • Address • Date of Birth • Contact Details • Country of residence and status
Financial Information	• Bank account details • Transactional details • Transactional history (statements etc)
Taxation	• Tax status • Tax domiciliation (where do you pay tax) • Copies of Tax returns
Family	• Number of dependents • Marital status • Lifestyle • Social circumstances
Financial Circumstances	• Personal wealth • Source of Wealth • Assets and liabilities • Proof of income • Expenditure • Credit history • Financial planning and objectives
Professional and Employment	• Previous and current employment details including • Term of employment – Part time/Full Time • Employer details • Salary
Visual	• Images and personal appearance • Copies of passports, ID cards, Drivers Licences, and other identification documents • CCTV images • Facial images • Voice recordings
Residential Details	• Address • Ownership status – homeowner/renting • Years of residence at address • Utility bills
Communications Data	• your communication preferences
Online Profile **(Based on your interactions with us, our website, online banking, and mobile app and subject to our Cookie Policy)**	• Activity • Internet Protocol (IP) address • smart device information • Location coordinates • Online and mobile banking security authentication • Mobile phone network information • Searches • Site visits • Spending patterns

3.3. Additionally, the bank may also collect, and process certain Personal Information categorised as "special category data". This may include information revealing:

- Your racial or ethnic origin
- Your religious or philosophical beliefs
- Your trade union membership
- Your health details and any medical conditions
- Your sex life or sexual orientation
- biometric information used for identification, fraud and money laundering prevention purposes including physical, physiological, and behavioural identifiers.
- criminal records of convictions and offences as well as allegations of criminal offences ("Crime Data")

3.4.

- We will not collect or use these types of data without your consent unless the law allows us to do so. If we do, it will only be when it is necessary:
    - Where we are obliged to do so as a matter of law or to comply with our legal or regulatory obligations, for example where we need to ensure that we have processed your information correctly, or to comply with our Know Your Customer (KYC) and anti-money laundering and counter terrorist financing obligations or if we need to forward information about you to a regulator; and
    - For reasons of substantial public interest for example, using Crime Data to help prevent, detect, prosecute financial crime, fraudulent behaviour, and unlawful acts.
        - To establish, exercise or defend legal claims.

4. WHY WE NEED THIS INFORMATION

4.1. In order to process your personal data, we need to have a legal and lawful reason for doing so under applicable data protection legislation.

4.2. The purposes include:

Purpose	Definition
Contractual Necessity	your Personal Data will be processed where it is necessary for performance of any contract with you for the provision of our products and services e.g., account onboarding, or to take steps at you request prior to entering into such a contract.
Compliance with legal obligations	The bank may be required to collect and process certain Personal Data in order to comply with relevant legislation (e.g., Anti-Money Laundering obligations). In these instances, we may be required to carry out additional and more detailed investigation into customer due diligence and subsequent reporting to regulators, authorities etc., particularly for the purpose of anti-money laundering, countering of terrorism finance and proliferation financing.
Protection of the bank's legitimate interests	We may collect and process your Personal Data where it is in our legitimate interests to do so and without prejudicing your interests or fundamental rights or freedoms. In this particular case, we will provide you with further details of those legitimate interests (e.g., our marketing communications will include this information).
Consent	We rarely rely on your consent to process your Personal Data, as usually another lawful basis will be more suitable. Where we do seek to rely on your consent, we will always ensure that this consent is fairly obtained by clearly informing you about why your consent is needed. Although consent can be obtained orally, we will usually require that you provide your consent through a clear, affirmative action such as ticking a box, toggling/swiping a button or switch on our website or on a mobile application, signing your name or other suitable method that can clearly evidence your consent. Non-exhaustive examples of when we may need your consent are: • To enable a feature on a mobile device application • To enable us to place cookies and similar technologies in accordance with our Cookie Policy • Where we rely on consent to send you marketing materials
Vital interests	The law allows us to process personal data where it is necessary to protect your vital interests or those of another person (e.g., matters of life and

	death). We rarely rely on this lawful basis, but it may apply in certain limited circumstances such as when we ask for allergy information or there is an incident at our premises.

5. HOW WE COLLECT AND PROCESS YOUR PERSONAL DATA

5.1. Personal Data is collected as follows:

Method	Definition
From you	• Completion of forms • Attending events • Visiting and interacting with our website • Attending meeting or speaking with our staff • Requesting information from us
From 3rd Parties	• Service providers • Government agencies • Other banks (where legally permitted) • Financial services providers • Regulatory authorities • Credit reference agencies • Due diligence and fraud prevention agencies
By us	• Information acquired and generated by us during the relationship including when you: o Apply for or use our products or services. o Use our Payment services. o Make enquiries with us. o make use Credit Card or Debit Card payments. o Access Online banking. o Use our website. o Call us (we record telephone calls for training, monitoring, or other legal/regulatory requirements).

6. WHAT DO WE USE YOUR PERSONAL DATA FOR?

6.1. Any information provided to us by you will be used for one or more of the following purposes:

- To provide services to you
- To meet legal, compliance and/or regulatory obligations
- To manage the relationship with you
- To perform financial crime risk management, including reporting suspicious activity to relevant authorities
- To enforce/defend the banks rights.
- To meet our internal policy requirements

We collect and use this Personal Data for the general purposes described in paragraph 6 and more particularly described in paragraph 7. If you do not provide Personal Data when we ask you for it, it may delay or prevent us from providing or continuing to provide our products or services t0 you.

7. WHAT WE USE YOUR PERSONAL DATA FOR IN MORE DETAIL

Purpose/reason	Lawful basis relied on	Relevant categories of Personal Data
To process your application for a product or service with us (including where you act on behalf of another e.g., through a Power of Attorney)	• Contractual Necessity • Consent (for biometric data)	• Basic Personal Information/Data, Taxation, Family, Financial Circumstances, Visual, Residential Details
To carry out identity checks, anti-money laundering checks and checks with due diligence and fraud prevention agencies (this will involve sharing your personal data with credit agencies and fraud prevention agencies)	• Compliance with legal obligation together with substantial public interest reasons	• Basic Personal Information/Data, Taxation, Family, Financial Circumstances, Visual, Residential Details,
Administering and managing your account and providing products and services (this may involve sharing your personal data with third parties including counterparties and others who assist us in providing you with our products and services). Communicating with you about such account's products and services.	• Contractual Necessity • Compliance with legal obligation together with substantial public interest reasons	• Basic Personal Information/Data, Financial Information, Taxation, Family, Financial Circumstances, Visual, Residential Details, Online Profile
To respond to any queries, you have in respect of our services and to fulfil the requests you make to us.	• Contractual Necessity	• Basic Personal Information/Data, Financial Information, Taxation, Family, Financial Circumstances, Visual, Residential Details, Online Profile
To collect and recover money owed to us (this may involve sharing your personal data with debt recovery agencies).	• Contractual Necessity • Necessary for our legitimate interests (to recover monies owed to us).	• Basic Personal Information/Data, Financial Information, Taxation, Family, Financial Circumstances, Residential Details, Online Profile
To perform checks and monitor transactions (including the use of location coordinates) to protect against fraud and complying with financial crime laws. This may require us to process Crime Data for the purposes of investigating and gathering intelligence on suspected financial crimes as well as sharing such data with law enforcement and regulatory bodies	• Compliance with legal obligation together with substantial public interest reasons • Consent (to track you when you enable this feature)	• Basic Personal Information/Data, Financial Information, Taxation, Family, Financial Circumstances, Visual, Residential Details, Online Profile
To administer and protect our business and our website and app (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	• Necessary for our legitimate interests for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise. • Necessary to comply with a legal obligation	• Financial Information, Online Profile

To exercise our rights and enforce the terms of our contract and to bring or defend legal claims	• Necessary for our legitimate interests to enforce our rights and protect our business	• Basic Personal Information/Data, Financial Information, Taxation, Family, Financial Circumstances, Visual, Residential Details, Online Profile
To ensure our internal processes and policies are adhered to	• Necessary for our legitimate interests to ensure our business is properly run in accordance with our policies and good governance. • Compliance with a legal obligation	• Basic Personal Information/Data, Financial Information, Taxation, Family, Financial Circumstances, Visual, Residential Details, Online Profile
To deliver relevant content to you and measure or understand the effectiveness of content the we serve to you	• Necessary for our legitimate interests (to study how customers use our interfaces products and services, to develop them, and to grow our business)	• Basic Personal Information/Data, Financial Information, Taxation, Family, Financial Circumstances, Visual, Residential Details, Communications Data, Online Profile
To use data analytics to improve our website, products/services, customer relationships and experiences	• Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, and to develop our business)	• Basic Personal Information/Data, Financial Information, Visual, Communications Data, Online Profile

8. SHARING YOUR PERSONAL DATA

8.1. We may access, preserve, and disclose to third parties' and independent correspondent banks information about you if we believe disclosure is in accordance with, or required by, any contractual relationship with you, applicable law, regulation, or legal process.

8.2. Personal Data may be processed by us internally and/or shared with third parties for the purposes specified in sections 6 and 7 or where you have consented to this, or if otherwise lawfully permitted.

8.3. Such third parties may include our affiliates, agents, vendors, consultants, or suppliers, as well as any other third-party service providers who are performing certain services on our behalf either as data processors, or as independent controllers such as lawyers, correspondent banks and other financial institutions and investment managers, hosted platform providers, third party screening providers and anti-fraud agencies, and debt recovery firms.

8.4. Where lawfully required, we may disclose Personal Data to relevant regulatory, law enforcement and/or other competent authorities including government entities, tax authorities, regulatory authorities, or trade bodies around the world.

8.5. We may also need to share your information in order to enforce or apply our legal rights under any agreed terms of business, including establishing, exercising, or defending legal claims, or in compliance with a legal, regulatory, or other administrative/judicial process (such as a court order).

8.6. The bank will not share your Personal Data with third parties for their own marketing purposes without your permission.

9. SHARING OR TRANSFERRING PERSONAL DATA OUTSIDE GIBRALTAR, THE UK AND THE EEA/EU

9.1. Countries outside Gibraltar, the UK and the EEA have differing data protection laws, some of which may provide lower levels of protection of privacy. It is sometimes necessary for us to transfer your personal data to countries outside Gibraltar, the UK and the EEA. In those cases, we will comply with relevant Gibraltar data protection laws designed to ensure the privacy of your personal data.

9.2. Under data protection laws, we can only transfer your personal data to a country outside Gibraltar, the UK and/or EEA where:

- the UK government has decided the particular country ensures an adequate level of protection of personal data (known as an 'adequacy regulation') further to Article 45 of the UK GDPR. A list of countries the UK currently has adequacy regulations in relation to is available here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for you; or

- a specific exception applies under relevant data protection law for example in order to provide you with a particular service such as making a payment to a non-Gibraltar, UK, or EEA country.

9.3. Where we transfer your personal data outside Gibraltar, the UK, or the EEA, we do so usually on the basis of an adequacy regulation or (where this is not available) through the use of legally approved standard data protection clauses recognised by the Gibraltar Regulatory Authority such as the Gibraltar International Data Transfer Agreement or Addendum. In the event we cannot or choose not to continue to rely on either of those mechanisms at any time, we will not transfer your personal data outside Gibraltar, the UK or EEA unless we can do so on the basis of an alternative mechanism or exception provided by relevant Gibraltar data protection laws and reflected in an update to this policy.

9.4. Any changes to the destinations to which we send personal data or in the transfer mechanisms we rely on to transfer personal data internationally will be notified to you in accordance with the section on 'Changes to this privacy policy' below.

10. YOUR RIGHTS

10.1. We want to make sure that you are aware of your rights in relation to the personal information and data we process about you.

10.2. Your data protection rights have been summarised for you below.

Access	The right to be provided with a copy of your Personal Data
Rectification	The right to require us to correct any mistakes in your Personal Data
Erasure (also known as the right to be forgotten)	The right to require us to delete your Personal Data in certain situations,
Restriction of processing	The right to require us to restrict processing of your Personal Data in certain circumstances, e.g., if you contest the accuracy of the data
Data portability	The right to receive the Personal Data you provided to us, in a structured, commonly used, and machine-readable format and/or transmit that data to a third party—in certain situations
To object	The right to object: • At any time to your Personal Data being processed for direct marketing or from (including profiling). • In certain other situations to our continued processing of your Personal Data, e.g., processing carried out for the purpose of our legitimate interests unless there are compelling legitimate grounds for the processing to continue or the processing is required for the establishment, exercise, or defence of legal claims
Not to be subject to automated individual decision making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you
The right to withdraw consents	If you have provided us with a consent to use your personal data, you have a right to withdraw that consent easily at any time. You may withdraw consents by letting us know by email. Please visit our website for the appropriate contact details. Withdrawing a consent will not affect the lawfulness of our use of your personal data in reliance on that consent before it was withdrawn

For more information on each of those rights, including the circumstances in which they apply, please contact us (see 'How to contact us' below) or see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights.

11. SECURITY

We are committed to ensuring that your information is secure with us and with the third parties who act on our behalf.

12. RETENTION PERIODS

12.1. We will retain your personal information only for as long as is necessary and for the purposes for which we process the information. Records can be held on a mixed variety of media (physical and electronic) and in varying formats.

12.2. Retention periods are determined by:

- the type of data record
- the nature of the record
- legal or regulatory requirements

12.3. justbank will, in the normal course of events, retain client records for up to a minimum of 7 years after the termination of our relationship. Subsequent to this period lapsing, your personal information will normally be destroyed. However, we may need to retain your Personal Information for a longer time period in cases where we are required to comply with legal or regulatory obligations, or in order to protect our interests or the interests of another natural person.

13. HOW WE PROTECT YOUR PERSONAL INFORMATION

The bank takes your privacy seriously and takes every reasonable measure and precaution to protect and secure your personal data. Our employees are trained on the importance of protecting your privacy and on the proper access restrictions, use and disclosure of personal data. We work hard to protect you and your data from unauthorised access, alteration, disclosure or destruction and we have implemented technical, organisational, and physical controls, safeguards and measures including:

Control	Purpose
Physical Access Controls	To prevent unauthorised persons from gaining access to data processing systems and include secure areas and equipment security. Physical access rights and authentication controls for secure areas have been implemented and documented and will be regularly reviewed and updated by central functions. We secure data on computer servers in a controlled, secure environment.
Logical Access Controls	To prevent data processing systems from being used without authorisation by way of personal login with a secure password that has to be changed periodically.
Data Access Controls	To ensure that persons with system access authorisation have access only to those data they are authorised to process and use. A process has been established to ensure that data is accessed only by those persons who are required to gain access for their work. Access is regulated by way of personal login with a secure password that has to be changed periodically and two factor authentication.
Disclosure Controls	To ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport, or while being recorded onto data storage media. State-of-the-art data transmission techniques are used that ensure (amongst other things) that it will be possible to check the recipient of the personal data transferred. Storage and transport precautions are taken to protect data media against damage or theft.
Input Controls	To ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered, or removed from data processing systems and if so, by whom. Logs are regularly evaluated by the person responsible for the system.
Job Controls	To ensure that personal data is processed strictly in compliance with our instructions. We take steps to ensure that any natural person or processor acting under our authority does not process data except on instructions from us (except as otherwise required by law).
Availability Controls	To ensure that personal data is protected against accidental destruction or loss, for instance by way of regular updates and storing of data on separate computer equipment or storage media.
Separation Controls	To ensure that data collected for different purposes can be processed separately by way of separating the access to the data.
Default Controls	To ensure that we only process your data which are necessary for each specific purpose of the processing, that wherever possible minimise the processing of your data and that transparency is maintained with regards to the functions and processing of your data.

Encryption Controls	To convert data into a code which makes it unreadable by anyone who might intercept it; including the use of 128-bit encryption on our online pages which hold your data, the pseudonymisation of data and the use Secure Socket Layer (SSL) encrypted protection to protect data.
Industry Controls	To ensure that our receipt and processing of certain payment data follow Industry standards.
Monitoring Controls	To enable us to constantly check the ongoing confidentiality, integrity, availability, and resilience of our processing systems. We routinely test and evaluate the effectiveness of our technical and organisational safeguards and measures
Your Online Security Controls	You must be responsible for protecting your own personal data, and we recommend that you keep your PC or device updated with anti-virus software, treat emails with caution (remember we will never ask you to disclose personal data via email) and ensure you choose a password that cannot be guessed easily.

Although we work hard to protect your data, no programme is one hundred per cent secure and we cannot guarantee that our safeguards will prevent every unauthorised attempt to access, use or disclose that data. The risks that may result from our processing of your personal data include identity theft or fraud, financial loss, loss of confidentiality, unauthorised reversal of pseudonymisation, and the inability to exercise control over your personal data. justbank maintains security and incident response plans to handle incidents involving unauthorised access to information we collect or store.

14. CHANGES TO THIS PRIVACY POLICY

We may update this Policy from time to time by publishing a new version on our website. When we make such changes or update this Policy, we may notify you of changes to this Policy by email (if you are a customer or are subscribed to our emailing lists) and will also update the "Last update" field at the top of this policy.

15. HOW TO CONTACT US

Individuals in Gibraltar

You can contact us and/or our Data Protection Officer by post or email if you have any questions about this privacy policy or the information we hold about you, to exercise a right under data protection law or to make a complaint.

Email - privacy@justbank.com

Address - 1 Montarik House, 3 Bedlam Court, Gibraltar GX11 1AA

16. HOW TO COMPLAIN

16.1. Please contact us if you have any queries or concerns about our use of your personal data (see below 'How to contact us'). We hope we will be able to resolve any issues you may have. You also have the right to complain to your local data protection supervisory authority.

16.2. In Gibraltar this is the GRA (https://www.gra.gi/)

justbank is a registered trading name of IDT Financial Services Limited a regulated bank, licensed by the Gibraltar Financial Services Commission. Registered Office: 57-63 Line Wall Road, Gibraltar. Registered No:95716.

IDT Financial Services Limited (trading as justbank) is covered by the Gibraltar Deposit Guarantee Scheme ('GDGS').

The GDGS can pay compensation to depositors if a credit institution is unable to meet its financial obligations. Ordinarily, most depositors – including individuals, corporations, and small businesses – can claim back up to EUR 100,000 of their deposits (or EUR 100,000 for each eligible account holder if it's a joint account). However, there are important exclusions which apply to certain depositors, which are set out on the website of the GDGS. For further information about the compensation provided by the GDGS refer to: www.gdgb.gi

If you are not satisfied with any of our products or services, we have a complaints procedure that you can use. A leaflet giving details of our complaints handling procedure is available from our website.

Calls may be recorded.