Justbank Privacy Notice

Contents

1. Who We Are

We are IDT Financial Services Limited trading as justbank (“**the bank**”, “**we**” or “**us**”).

We are regulated and authorised by the Financial Services Commission, Gibraltar.

We gather and process your personal data in accordance with this notice and in compliance with all relevant local and international **data protection legislation** and regulations.

This notice provides you with the necessary information regarding your rights and our obligations, and explains how, why, and when we process your data. We are committed to protecting the privacy of your data.

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).

We are a **data processor** in respect of the processing of your data, and when we use other data processors who act on our instructions.

We respect individuals’ rights to privacy and to the protection of personal information and committed to protecting the privacy of your data.

Reference to “**Personal information**” and “**Personal Data**” relates to information and/or data about a living individual who can be identified from that information (either by itself or when it is combined with other information).

This Privacy Notice should be read in conjunction with our Terms & Conditions and other contractual documentation and agreements.

We have a separate Cookie Policy specific to the use of our website – www.justbank.com

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	Information and/or data about a living individual who can be identified from that information (either by itself or when it is combined with other information).
Data Subject	Any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity. In other words, a data subject is an end user whose personal data can be collected.
Data Controller	Any organisation, person, or body that determines the purposes and means of processing personal data, controls the data and is responsible for it, alone or jointly. Examples when the data controller is an individual include general practitioners, pharmacists, and politicians, where these individuals keep personal information about their patients, clients, constituents etc. Examples of organizations can be data controllers, for profit or not for profit, private or government-owned, large, or small, where those organizations keep personal information about their employees, clients, etc.
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. It offers privacy protections and guarantees in a similar manner. Following an agreement on Gibraltar between the UK and the EU, the Gibraltar GDPR was amended to re-instate the EU GDPR, albeit still with some derivations.
Data Protection Act 2004	Gibraltar specific Data Protection Legislation.
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
Data Protection Legislation	Data Protection laws and regulations including EU GDPR, Gibraltar GDPR and Data Protection Act 2004.
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 members of the EEA.
PCI DSS	An industry security standard applicable to entities and environments that store, process or transmit payment card account data, including cardholder data and sensitive authentication data.

3. The Information We Process

The Bank collects and processes various categories of personal information at various stages of our relationship with you, 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.

The types of personal information (and examples of these) we collect may include (and this is not an exhaustive list) are listed below. In some instances, the Bank 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 Education	• Education and qualifications • 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
Online profile & social media (Based on your interactions with us, our website, online banking,	• Activity • Internet Protocol (IP) address • smart device information

and mobile app and subject to our Cookie Policy)	• Location coordinates • Online and mobile banking security authentication • Mobile phone network information • Searches • Site visits • Spending patterns

Additionally, the Bank may also collect, and process certain personal information categorised as "sensitive data". In these instances, the information will be collected for specific and limited purposes, such as detecting and preventing financial crime or to make our services accessible to customers. The Bank will only process special categories of information where your explicit consent has been obtained or are otherwise lawfully permitted to do so (and then only for the particular purposes and activities for which the information is provided). 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

Where permitted by law the Bank may process information about criminal convictions, criminal offences, related security details, alleged offences including unproven allegations, spent or previous convictions, or other details provided in relation to a criminal reference check or similar.

4. Why We Need This Information

In order to process your personal data, we need to have a legal and lawful reason and purpose for doing so as defined under Data Protection Legislation which justifies the processing.

The purposes included:

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 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, which may extend beyond the Data Protection 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). Additionally other legitimate interests include: • Exercise, establishment or defence of legal claims • To prevent fraud • Maintain the security of bank assets and staff • Assist police and authorities in disclosing criminal acts e.g., CCTV • Employee monitoring – employees are subject to separate Privacy Notice
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
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.
Public interest	When processing more "sensitive" types of Personal Data, we will rely on one of the above lawful bases together with additional safeguards and lawful bases required in respect of this data. We will inform you of these as appropriate

5. How We Collect And Process Your Personal Data

Personal Data is collected as follows:

Method	Definition
By you	• Completion of forms • Attending events • Visiting and interacting with our website • Attending meeting with our staff • Requesting information from us
3rd Parties	• Service providers • Government agencies • Other banks (where legally permitted) • Financial services providers • Regulatory authorities • Credit reference agencies
By us	• Information acquired and generated by us during the relationship including: ○ Our services ○ Payment services ○ Enquiries ○ Credit Card or Debit Card payments ○ Online banking ○ Website ○ Mobile app ○ Telephone recordings for training, monitoring or other legal/regulatory requirements. ○ Job applications

6. What Do We Use Your Personal Data For?

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

- To provide services to you
- To manage the relationship with you
- To meet legal, compliance and/or regulatory obligations
- 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
- To market our products and services to you

7. Sharing Your Personal Data

We may access, preserve, and disclose to third parties' 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.

Personal Data may be processed by us internally and/or shared with third parties for the purposes specified above, where you have consented to this, or if otherwise lawfully required.

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 (as data processors), such as lawyers, correspondent banks and other financial institutions, investment managers or other service providers.

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.

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).

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

8. Sharing Or Transferring Personal Data Outside Gibraltar and the EEA/EU

This will be done in the following conditions:

- IT development, hosting, and support
- payment service provision to its customers
- human resources/talent acquisition

Personal Data is transferred to data processors within and outside of the EEA (the EEA includes countries in the European Union as well as Iceland, Lichtenstein, and Norway). Under Gibraltar GDPR, all transfers outside of Gibraltar are treated as transfers to a "third country" as that expression means a country or territory outside of Gibraltar.

In cases where we intend to transfer personal data to third countries or international organisations outside of Gibraltar, we are required to confirm to you whether it has been determined by under Gibraltar GDPR that the country or organisation we are sharing your Personal data with will protect your information adequately. Specifically, we need to confirm the existence or absence of a decision based on an adequacy regulation as set out in Article 45(1) of the Gibraltar GDPR (known as a "adequacy regulations" made by the United Kingdom).

The requirements are that these countries provide the following safeguards:

- Binding corporate rules
- Standard data protection clauses specified in regulations made under the Data Protection Legislation
- Approved codes of conduct
- Approved certification mechanisms

In the absence of adequacy regulations or appropriate safeguards, we may rely on derogations for specific situations and perform transfers which are necessary for a defined set of reasons (e.g., performance of a contract between the Bank and the data subject, or to implement pre-contractual measures), or where you give explicit consent to the transfer.

Finally, we may also perform such transfers in 'one-off' cases where a transfer is not repetitive, concerns a limited number of data subjects, and is necessary for the purposes of compelling legitimate interests pursued by the Bank.

9. Your Rights

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

Your rights under existing Data Protection Legislation have been summarised for you below.

Right	Description
Confirmation & Access *The right to have access to the personal information we hold about you*	You have the right to ask us to confirm to you whether or not we collect, process, or store your Personal Data. Where we collect process or store your Personal Data, you are entitled to access to your Personal Data, and you further have the right to be informed about: • the purposes of the processing. • the categories of Personal Data concerned. • the envisaged period for which the Personal Data will be stored or if not possible, the criteria used to determine that period. • the existence of the right to request from us rectification or erasure of Personal Data, or restriction of processing of Personal Data concerning you as a Data Subject, or to object to such processing • the existence of the right to lodge a complaint with a regulator • where the Personal Data is not collected from you, any available information as to its source • the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for you • whether your Personal Data is transferred to a third country and if so of the appropriate safeguards relating to the transfer Note: most of this information is already contained within our Privacy Notice. Exercising this right is also referred to as submitting a “data subject access request” or “DSAR”.
Rectification *The right to rectification of inaccurate personal information and to update incomplete personal information*	You have the right to have any inaccurate Personal Data about you rectified and to have any incomplete Personal Data about you completed. It is important that the Personal Data we hold about you is accurate and current. Any terms and conditions which we may have with you will also require you to inform us if your Personal Data changes during your relationship with us. If we do hold Personal Data and you believe it is incorrect, you may submit a request to us to correct any alleged mistakes. We shall communicate any rectification of Personal Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort, and shall inform you about such recipients if you request this information.
Erasure (be ‘forgotten’) *The right to request that we delete your personal information*	You have the general right to request the erasure of your Personal Data. This right can be exercised if one of the following applies: • the Personal Data is no longer necessary for the purpose it was collected for.

	• you withdraw your consent-to-consent based processing and no other legal justification for processing applies. • you object to processing for direct marketing purposes. • we unlawfully processed your Personal Data; and/or • erasure is required to comply with a legal obligation that applies to us. Once you have requested erasure of your Personal Data for one of the reasons above, we will proceed to comply without delay unless continued retention is necessary for: • exercising the right of freedom of expression and information. • complying with a legal obligation under EU or other applicable law. • the performance of a task carried out in the public interest. • archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, under certain circumstances; and/or • the establishment, exercise, or defence of legal claims. • We shall communicate erasure of Personal Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort, and shall inform you about such recipients if you request this information.
Right	**Description**
Restriction of processing *The right to request that we restrict the processing of your personal information*	You have the right to restrict the processing of your Personal Data under certain circumstances. You may restrict the processing of your Personal Data when: • you contest the accuracy of the Personal Data • processing is unlawful you may request, but you do not want us to erase it • we no longer need to process your Personal Data, but you need the Personal Data for the establishment, exercise, or defence of legal claims • you object to processing that relies on the public interest or on our legitimate interests as the lawful processing grounds, and in this case, we must restrict the challenged processing activity pending the verification of whether our legitimate interests override your interests. • we shall communicate restriction of processing of Personal Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort, and shall inform you about such recipients if you request this information
Data Portability *The right to data portability*	You have a right to receive the Personal Data concerning you (which you have provided to us) in a structured, commonly used, and machine-readable format, or ask us to send it to another person where this is technologically possible. This right only applies where: • processing is based either (i) on your consent or (ii) on a contract we have with you (or steps taken at your request prior to entering into a contract); and • processing is carried out by automated means (i.e., excluding paper files). Processing by automated means is understood as general electronic processing and is to be

	distinguished from automated decision-making (explained below). This right does not include any additional data that created by us based on the data you have provided. For example, if we use the Personal Data you have provided to create a user profile, then this Personal Data would not be in scope of data portability (but could be in the scope of a data subject access request as explained above). Additionally, if we are not responsible for the privacy practices of others where you ask us to port your data to a third party.
Objection to processing *The right to object to the processing of your personal information*	You have a right to object to us processing your personal information (and to request us to restrict processing) unless we can demonstrate compelling and legitimate grounds for the processing, which may override your own interests or where we need to process your information to investigate and protect us or others from legal claims. Depending on the circumstances, we may need to restrict or cease processing your personal information altogether, or, where requested, delete your information. Please note that if you object to us processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.
Marketing (opting out) *The right to object to direct marketing*	You have a right to object at any time to processing of your personal information for direct marketing purposes, including profiling you for the purposes of direct marketing.
Withdraw consent *The right to withdraw consent*	Where we rely on your permission to process your personal information, you have a right to withdraw your consent at any time. We will always make it clear where we need your permission to undertake specific processing activities.
Right	**Description**
Lodge Complaint *The right to lodge a complaint*	If you wish to raise a complaint on how we have handled your personal information, you can contact our Data Protection Officer: privacy@justbank.com 3rd floor, 10 Cannon Ln, Gibraltar GX11 1AA Alternatively, you have the right to make a complaint on how we have handled your personal information to the Data Protection regulator – The Gibraltar Regulatory Authority (GRA). www.gra.gi/data-protection/complaints
Freedom from automated decision making *The right to request that decisions made about you using your personal data are made by humans*	You have a right data not to be subject to a decision based solely on automated processing (i.e., by computers and without human intervention), including profiling, which produces legal effects concerning you or similarly significantly affects you. However, this right does not apply when the decision: • Is necessary for entering into, or performance of, a contract between you and the Bank • Is required or authorised by law

	• Is based on your explicit consent Although certain third parties (e.g., credit referencing agencies) may use automated decision-making tools or software, we do not use automatic decision-making or profiling when processing personal data. If this changes, we will confirm this to you and provide meaningful information about the logic involved, as well as the significance and the envisaged consequences for you.

10.Security

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

11.Retention Periods

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.

Retention periods are determined by:

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

The Bank will, in the normal course of events, retain client records for up to a minimum of 10 years after the termination of our relationship. Subsequent to this period lapsing, your personal information will 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 your interests or the interests of another natural person.

12.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. The Bank maintains security and incident response plans to handle incidents involving unauthorised access to information we collect or store.

13. Card and Payment Information

We collect and use information relating to your payment cards, transactions and associated payment services in order to provide and administer your account and card services, process and verify transactions, prevent and detect fraud, manage security risks, comply with our legal and regulatory obligations and protect our customers and our business.

13.1. Information we may hold

Depending on the products and services you use, this may include information relating to your payment card and its lifecycle, such as:

- your name and other customer identification information;
- your payment card number or other card identifier;
- card expiry date and status;
- information relating to the issue, personalisation, delivery, activation, replacement and cancellation of your card;
- payment and transaction information; and
- information relating to the use and security of your card.

We only collect, process and retain information that is necessary for the relevant purpose and in accordance with applicable legal, regulatory and security requirements.

13.2. How we protect your card and payment information

We maintain technical, physical and organisational security measures designed to protect your personal and card-related information against unauthorised access, loss, theft, misuse, alteration or disclosure.

Physical payment cards and card stock are handled through controlled processes designed to protect cards throughout their lifecycle, including manufacture, personalisation, storage, transportation, delivery, replacement, cancellation and secure destruction.

Access to card stock, card-related information and payment information is restricted to authorised personnel and approved service providers who require access for legitimate business purposes.

13.3. Payment card security standards

Where applicable to the relevant payment-card environment, we maintain controls designed to meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS is an industry security standard applicable to entities and environments that store, process or transmit payment card account data, including cardholder data and sensitive authentication data. It is not a certification covering all personal information held by the Bank.

Where relevant, our payment-card environments are assessed against the applicable PCI DSS requirements.

13.4. Storage and retention of card information

We retain cardholder and payment information only for as long as necessary to provide our services and for legitimate business, legal, regulatory, fraud-prevention, dispute-resolution, accounting, audit and security purposes.

Where cardholder data is stored, we apply appropriate security controls and access restrictions. Payment card information is not retained simply because it has been collected; retention is subject to our applicable data-retention requirements.

Certain sensitive authentication information is subject to additional restrictions under applicable payment-card security requirements. For example, card verification codes are not retained after the relevant authorisation process, except where a specific PCI DSS provision applicable to card issuers or issuing services permits such retention.

13.5. Card and payment service providers

We may use specialist service providers to support the manufacture, personalisation, processing, delivery, administration, security and secure destruction of payment cards and related information.

Where we use such providers, we require appropriate contractual, technical and organisational safeguards to protect your information. Depending on the service provided, this may include requirements relating to PCI DSS, information security, access controls, confidentiality, data retention, secure destruction and incident management.

13.6. Secure disposal

When card stock, card-related records or payment information are no longer required, we take appropriate measures to securely delete, destroy or otherwise dispose of them in accordance with our retention and security requirements.

Further information about how we protect your card and security information, including steps you can take to protect your card, is available on our **Card Security** webpage.

14. Data Breaches

A loss of Personal Data is known as a data breach. The GDPR imposes requirements on businesses to identify, assess and report breaches in a timely manner (within 72 hours). We undertake to inform you if your Personal Data is compromised and there is a high risk to your rights and freedoms as a result.

15. 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. If you do not have a business relationship with us, you are encouraged to review our website regularly in order to remain informed about how we process Personal Data.

From time to time, we may update our Privacy Notice. We will communicate these changes to you directly and/or by publishing the updated Privacy Notice on our website www.justbank.gi/privacynotice. We recommend that you to visit our website regularly to stay informed of any changes.

In respect of any personal information relating to a third party that you provide to us, you must:

a) notify the third party that you are providing their personal information to us and obtain their permission.
b) provide the third party with a copy of our Privacy Notice and these Terms and Conditions
c) promptly notify the third party of any changes to our Privacy Notice that we notify you of;
d) ensure that, to the best of your knowledge, the personal information is accurate and up to date, and promptly notify us if you become aware that it is incorrect.

We will only share your information where it is necessary for us to carry out our lawful business activities, or where it is necessary to comply with laws and regulations that apply to us.

We will not share your information with anyone outside justbank except:

a) Where we have your permission.
b) Where required, whether directly or indirectly, for your product or service, which could include in relation to your welfare or accessibility requirements.
c) Where permitted by law, or it is necessary for our legitimate interests or those of a third party, and it is not inconsistent with the purposes listed below
d) In anonymised form as part of statistics or other aggregated data shared with third parties
e) Where required for a proposed sale, reorganisation, transfer, financial arrangement, asset disposal or other transaction relating to our business and/or assets held by our business.

This is a list of examples of 3rd parties we could potentially have a requirement to share your information with and rationale for this:

3rd party class	3rd party type	Rationale
Legal and regulatory	Law enforcement agencies Judicial bodies Government entities Tax authorities Regulatory bodies Regulators	To comply with legal or regulatory requirements To ensure contractual rights or obligations relating to products or services provided to you are in line with existing legislation and regulations
Financial	Other banks Payment service providers	To recover funds if these have been sent to you in error
Prevention of crime/money laundering	Other banks Regulators Law enforcement	In the event of suspected fraud or financial crime or criminal activities For monitoring, prevention, and investigation of suspected fraud or financial crime or criminal activities
Operational	Other banks Market analysts Sub-contractors	Our service providers such as correspondent banks, printers, market analysts etc
Marketing	Social media companies Advertisers	Always in secure format and depersonalised so they can display or send relevant messages to you and others or compile information relevant to marketing to you about our products and services on our behalf. Third party advertisers may also use information about your previous web activity to tailor adverts which are displayed to you.
Credit	Debt collection agencies Credit reference agencies	Collection of debt

If you ask us to, we will share information with any third party that provides you with account information or payment services. If you ask a third-party provider to provide you with account information or payment services, you're allowing that third party to access information relating to your account. We're not responsible for any such third party's use of your account information, which will be governed by their agreement with you and any privacy statement they provide to you.

If any additional authorised users are added to your account, we may share information about the use of the account by any authorised user with all other authorised users.

We will not share your information with third parties for their own marketing purposes without your permission.

We may transfer your information to organisations in other countries on the basis that anyone to whom we pass it protects it in the same way we would and in accordance with applicable laws. If we transfer information to countries outside of the European Economic Area (which includes countries in the European Union as well as Iceland, Liechtenstein, and Norway) or the jurisdictions we operate in, we will only do so where:

a) The European Commission has decided that the country or the organisation we are sharing your information with will protect your information adequately.
b) The transfer has been authorised by the relevant data protection authority; and/or
c) We have entered a contract with the organisation with which we are sharing your information (on terms approved by the European Commission or the Data Protection Authorities in the jurisdictions we operate in) to ensure your information is adequately protected.