Gibraltar INTERNATIONAL BANK

Privacy Policy

1. Introduction & Scope of this Privacy Policy

Protection of your privacy and the security of your personal data are very important to us. The Bank (defined below) collects and processes personal data and we are required to inform you how and when we collect, process, share and/or disclose your personal data.

This Privacy Policy (this "**Policy**") sets out what personal data we collect, how we process it and how long we generally retain it, along with details of your rights as a data subject. Together with our Cookie Policy (https://www.gibintbank.gi/terms) and Website Terms & Conditions (https://www.gibintbank.gi/terms), this Policy applies to all users of our website https://www.gibintbank.gi, as well as our customers/clients.

If you are just browsing, we have designed our website so that you may navigate and use it without having to provide Personal Data, subject only to certain data that may be collected via the use of cookies.

If you do not accept these policies, you should immediately discontinue your use of our website.

This Policy also is intended to apply to our clients/customers, who are also subject to the General Terms and Conditions of the Banking services we provide (https://www.gibintbank.gi/termsgib), as well as users of our website (irrespective of whether they use our services). To the extent that you are a customer or user of our services, this Privacy Policy applies together with any Terms of Business and other contractual documents, including but not limited to any agreements we may have with you.

In this Policy, "**personal data**" means any information relating to you as an identified or identifiable natural person ("**data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an online identifier or to one or more factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity. For the avoidance of doubt, personal data does not include data from which you cannot be identified (which is referred to simply as data, non-personal data, anonymous data, or de-identified data).

In this Policy, "**processing**" means 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. Likewise, "**process**" shall be interpreted accordingly.

If we determine the purposes and means of processing of your personal data, then we are a "**controller**", and anyone who acts on our instructions in respect of such processing is a "**processor**". There may be times where we act as controller and processor.

For avoidance of doubt, this Policy is not intended to cover our privacy obligations towards our employees (including consultants) or prospective employee, which are explained within our Employee Privacy Policy and Recruitment Privacy Policy, respectively. Such policies will be made available during the application process and at commencement of employment, where applicable. We reserve our right to issue separate policies in respect of other relevant stakeholders such as our employees, prospective employees connected persons, affiliates and/or our business partners.

We offer services in or from within Gibraltar, which is no longer part of the EU. Accordingly, Gibraltar has its own data protection laws that apply certain EU laws. This is referred to as the "**Data Protection Legislation**", which includes:

- The Data Protection Act 2004 (as amended)("**DPA 2004**"), and regulations made under that Act; and
- The "**Gibraltar GDPR**", which is essentially the EU's General Data Protection Regulation or (Regulation (EU) 2016/679, or the "**EU GDPR**") as it forms part of Gibraltar law. This basically means it is read slightly differently to the EU GDPR but still offers privacy protections and guarantees in a similar manner.

If you live or work outside of Gibraltar, other laws, including the EU GDPR, may be applicable to your individual circumstances.

2. Who we are and how to contact us

In this Policy, "**we**", "**us**" and "**our**" refers to Gibraltar International Bank Limited (the "**Bank**").

If you would like to exercise any of the rights explained below, or if you have any questions regarding this Policy or generally about the way we handle your personal data, write into us at:

Data Protection Officer
Gibraltar International Bank Limited
Ince's House
310 Main Street
Gibraltar, GX11 1AA

Tel: +350 (200) 13900
Email: dpo@gibintbank.gi

3. What personal data do we collect and process?

The Bank collects and processes various categories of personal data at the start of and for the duration of our relationship with you. Some categories of personal data are kept beyond the termination of our relationship where so required and there is a legitimate purpose for doing so. We limit the collection and processing of information to what is necessary to achieve one or more of the lawful bases identified in this Policy.

Personal data which we may collect and process may include:

(a) basic personal data, such as name and address, contact details and date of birth;
(b) financial history and information, such as transactional information, proof of income, personal wealth, assets and liabilities, credit history, details of expenditure and outgoings;
(c) information about the purpose and scope of your expected relationship with the Bank;
(d) basic information about your family, partners and dependants and your social circumstances;

(e) employment history;
(f) personal identification documents, such as copies of passports etc.;
(g) Online profile and social media information obtained as a result of use of the Bank's websites, platforms and applications, such as the Internet protocol address and any other similar data and information that may be used in the event of attacks on our information technology systems (see further information on our Cookie Policy).

Additionally, we may also process certain special categories of data. This data would only be collected and processed with either your explicit consent or where we are lawfully permitted to do so without your consent (e.g., personal data which is manifestly made public by you). Such processing would be for limited purposes such as fraud prevention, prevention of money laundering, financial crime and terrorist financing. Such data may include matters such as:

(a) racial or ethnic origin;
(b) political opinions
(c) religious or philosophical beliefs;
(d) trade union membership;
(e) health or medical conditions (physical or psychological);
(f) sex life or sexual orientation
(g) criminal convictions (including the alleged commission of offences, proceedings in relation to such offences or alleged commission of offences or the disposal of such proceedings, including sentencing).

We do not process genetic data or biometric data for the purpose of uniquely identifying you, and this would only be considered for our employees whom are covered by a separate privacy notice.

4. How do we collect your personal data?

We collect your personal data in the following manner:
(a) Information you provide to us directly when contacting us or meeting us at our offices;
(b) Information we receive from third parties, such as third party service providers, government agencies/departments and other banks, financial services institutions and regulatory authorities;
(c) Information acquired by us during the course of our relationship and dealings with you;
(d) Information collected through the use by you of our website, platforms and applications;
(e) Information that may be collected as a result of the recording of telephone conversations or CCTV footage;
(f) Information gathered from publicly available sources.

5. The purposes for which we process your personal data as well as the legal basis for the processing

In order to process personal data, we need a valid lawful basis under the Data Protection Legislation which will justify the processing. The purposes for which your personal data is collected and processed include the following.

Contractual necessity

This lawful basis applies to most of our processing activities in relation to personal data belonging to our customers/clients. It applies both during the pre-contractual stages of our banking relationships as well as once the contractual agreement(s) are in place.

Compliance with a legal obligation to which the Bank is subject

Certain laws and regulations, other than the Data Protection Legislation, may require us to process personal data. For example, we are required to retain information in accordance with record-keeping requirements under applicable legislation. Further we may need to carry out certain investigations, customer due diligence, and reporting for the purposes of anti-money laundering (including counterterrorist and proliferation financing) legal and/or regulatory requirements.

Legitimate interests of the Bank or a third party

We may also process your personal data where it is in our legitimate interests (or the interests of a third party) to do so, provided that those interests override your interests or fundamental rights or freedoms. There may be cases where your interests and fundamental rights could override our legitimate interests. This may happen in cases where personal data are processed in circumstances where you do not reasonably expect further processing. We will always need to (i) *identify* a legitimate interest (ii) show that processing is *necessary* to achieve it; and (iii) *balance* it against your interests, rights and freedoms. Some non-exhaustive examples of situations where we may seek to pursue legitimate interests are:

- for marketing purposes;
- for the exercise, establishment or defence of legal claims;
- to prevent fraud, keep our staff and premises secure and disclosing criminal acts (e.g. CCTV use);
- employee monitoring (to which our employee privacy notice(s) will apply); and/or

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; or
- 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.

Task carried out in the public interest or to exercise official authority

Given it is more relevant to public authorities, we will not normally rely on this lawful basis, and will inform you if this changes.

6. What do we use your personal data for?

We will only use and share your information where it is necessary and lawful for us to do so in carrying on our business. The personal data we collect from you may be used in one or more of the following ways:

- To provide our services to you;
- To manage your relationship with us;
- To meet legal, compliance and or regulatory obligations;
- To perform financial crime risk management and assessment;
- To enforce/defend our rights;
- To meet our internal policy requirements;
- To market our products to you.

7. Sharing your personal data

Personal data may be processed by us and/or our affiliates, agents, vendors, consultants or suppliers, as well as any other third party service providers who are performing certain services on our behalf for the purposes specified above or on your instructions. 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.

The Bank discloses information to external business partners (including correspondent banks and other financial institutions) where it has a lawful basis to do so. For example, your personal data may be disclosed if we enter into a sale, reorganisation, transfer or asset disposal with or merge with another business entity, in which case it may be disclosed to that entity. In addition, we may be required by law or by a court of law to disclose personal data to relevant regulatory, law enforcement and other competent authorities.

Transferring your personal data outside of Gibraltar and the EEA

In connection with IT hosting and support, personal data is transferred to data processors, including data processors in '*third countries*' outside the European Economic Area ("**EEA**") (which includes countries in the European Union as well as Iceland, Lichtenstein and Norway), such as Dubai.

Such transfers of personal data to third countries or international organisations are referred to as '*restricted transfers*', as they require justification under the Data Protection Legislation. Note that transfers to the United Kingdom are not restricted in this manner.

Generally, we will only perform restricted transfers where the transfer will be adequately protected by measures such as the following:

- where the transfer is to a territory that has been deemed 'adequate' under the Data Protection Legislation, through applicable adequacy regulations;
- where 'appropriate safeguards' are provided such as:
    - 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.

8. Storing personal data

We retain personal data only for as long as is necessary for the purposes for which we process the information as set out in this Policy. Records can be held in a variety of ways (physical or electronic) and formats.

Retention periods are determined based on the type and nature of the information and the legal or regulatory requirements that apply. We will, in the normal course of events, keep client records for up to six years after the termination of the relationship. However, we may retain your personal data for a longer period of time where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

9. Your rights as a data subject

We are required to inform you about your rights under the Data Protection Legislation and provide information on these below. If you wish to exercise any of these rights, please contact our data protection officer ("**DPO**") on the details provided in this Policy. We may need to request specific information from you to help us understand the nature of your request, to confirm your identity and to ensure that Personal Data is not disclosed to any person who has no right to receive it. Requests will be processed within one month of receipt, but this might be extended by two further months in case of a complex request, where you have made a number of requests, or if the identity of the requestor cannot be verified. We will not normally charge a fee for actioning such requests but may charge a reasonable fee where one or more of your requests are manifestly unfounded or excessive, in particular because any repetitive character in such requests. In such cases we may also refuse to comply with such requests.

We shall communicate restriction, rectification or 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.

Depending on your particular circumstances, you may also have additional rights if you live or work outside of Gibraltar. For example, the EU GDPR may apply to you if you are based in the EEA.

The right to confirmation and access

You have the right to ask us to confirm to you whether or not we collect, process or store your personal data (also known as a "**data subject access request**" or "**DSAR**"). You have the right to be informed about:

- the purpose of the processing we do;
- the categories of personal data we hold;
- the envisaged period for which it 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 or to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- 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; and
- whether your personal data is transferred to a third country and if so of the appropriate safeguards in place relating to the transfer.

Note that most of the above information is already contained in this Policy.

The right to rectification

You have the right to have any inaccurate personal data about you rectified and to have any incomplete personal data about you completed. You may also request that we restrict the processing of that information. If you ask us to restrict processing we may have to suspend the operation of some or all of our services to you.

The right to erasure

You have the general right to request the erasure of your personal data in the following circumstances:

- the personal data is no longer necessary for the purpose for which it was collected;
- 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; or
- erasure is required to comply with a legal obligation that applies to us.

We will proceed to comply with an erasure request 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 defense of legal claims.

The right to restrict processing

You have the right to restrict the processing of your personal data under certain circumstances:

- you contest the accuracy of the personal data;
- where processing is unlawful you may request, instead of requesting erasure, that we restrict the use of the unlawfully processed personal data;
- we no longer need to process your personal data but need it for the establishment, exercise, or defense of legal claims.

If you ask us to restrict processing we may have to suspend the operation of some or all of our services to you.

The right to object to processing

You have the right to object to processing of your personal data under certain circumstances, these include:

- where we rely on legitimate interests as the lawful basis
- where our processing is for direct marketing purposes (including profiling for direct marketing purposes);
- where processing is for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation. Note the Bank does not process your personal data for these purposes; or
- where processing is based on performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. We have noted above that we do not rely on this lawful basis, which mostly applies to public authorities.

Where you object on the above basis, we will cease to process your personal data unless there are compelling legitimate grounds for processing which override your interests, or we need to process your personal data to establish, exercise, or defend legal claims.

The right to data portability

Where the legal basis for our processing is your consent or is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, you have a right to receive the personal data you provided to us in a portable format. Additionally, you may also ask us to provide it directly to a third party and we will do so where this is feasible. The Bank is not responsible for the use for any third party's use of that information. Note that this right only applies where 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). Further, this right does not include any additional data that is created by us based on the data you have provided.

The right to withdraw consent

Where the legal basis for processing your personal data is your consent, you have the right to withdraw that consent at any time (without affecting the lawfulness of processing based on consent before its withdrawal). Consent should be as easy to withdraw as it is to give, so we will normally provide toggle switches, tick boxes or forms that allow you to change your preference at any time online. However, you may also contact our DPO in order to exercise this right (as well as any other rights).

The right to complain to a supervisory authority

If you consider that our processing of your personal data has infringed data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. If you are outside of Gibraltar, you may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement. We encourage you to contact our DPO on the above details prior to raising a complaint, as the Bank may be able to directly address your complaint. If you remain unsatisfied, you are entitled (regardless of where you are based) to make a complaint to the

Information Commissioner under the DPA 2004, which is presently the Gibraltar Regulatory Authority ("**GRA**"). You may contact the GRA on the below details:

Address: Gibraltar Regulatory Authority, 2nd Floor, Eurotowers 4, 1 Europort Road, Gibraltar
Email: info@gra.gi
Phone: (+350) 200 74636
Fax: (+350) 200 72166
Website: www.gra.gi

Right to freedom from direct marketing (opting-out)

You have an absolute, unqualified right to freedom from direct marketing also referred to as '*opting out*'. You can exercise the right at any time by contacting our DPO, but we will also provide 'unsubscribe' options in our electronic marketing material. Where you exercise opt-out, we may need to retain your details to ensure we do not send you further marketing.

10. Existence of automated decision-making

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; or
- 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.

11. How we secure your information

We are committed to taking appropriate measures designed to keep your personal data secure from loss, theft, misuse and accidental, unlawful or unauthorised access, disclosure, alteration, use and destruction. We follow generally accepted standards to protect the personal data submitted to us, both during transmission and once it is received. We update and test our security technology on an ongoing basis.

Access to your personal data is restricted to those employees who need to access that information to provide our services to you. Furthermore, we train our employees about the importance of confidentiality and maintaining the privacy and security of your information.

As explained in this Policy, our website does collect your personal data. More information is found in our Cookie Policy https://www.gibintbank.gi/terms

12. Data breaches

The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data is known as a "**data breach**". The Gibraltar GDPR imposes certain requirements on controllers to identify, assess and report data breaches in a timely manner. Where we have to provide a notification to the GRA, this shall be done without undue delay and, where feasible, not later than

72 hours after we became aware of a data breach. Where the notification to the GRA is not made within 72 hours, it will be accompanied by reasons for the delay.

We undertake to inform you, when required, if your personal data is compromised and there is a high risk to your rights and freedoms as a result.

13. 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 updated" 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

14. Limits to your right to information

Your right to information under Art. 13 and 14 of the Gibraltar GDPR is limited in certain cases. The requirements to give information do not apply insofar as:

- The provision of information to you proves impossible or would require disproportionate effort on our part in order to provide. This is provided that we take appropriate steps as controller to protect your rights as a data subject, your freedoms and your legitimate interests, including by making information publicly available (as this Policy intends to do);
- obtaining or disclosure is expressly laid down by Gibraltar law which we are subject and which provides appropriate measures to protect your legitimate interests;
- the personal data must remain confidential subject to an obligation of professional secrecy regulated by Gibraltar law (such as statutory obligations of secrecy); or
  you already have the information.