Whistleblowing Privacy Statement

This is our statement about what we do with your personal data and our legal right for doing it.

We respect your privacy and are committed to protecting your personal data when you are supplying us with information.

Our overall purpose is to regulate the financial services industry in Gibraltar in the public interest. Our aim is to protect consumers, enhance the reputation of Gibraltar as a quality financial services centre and promote good business practices. Our activities involve three core areas, which are Authorisation, Supervision and Enforcement.

1. IMPORTANT INFORMATION AND WHO WE ARE

PURPOSE OF THIS PRIVACY POLICY NOTICE

It is important that you read this privacy policy together with any other privacy notice or data processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using data about you. This privacy policy supplements any such other notices and is not intended to override them.

DATA PROTECTION LAW

How Gibraltar companies deal with your personal data is governed by the Data Protection Regulation (EU 2016/679) (GDPR). EU regulations are directly applicable in EU member states. GDPR seeks to harmonise privacy laws across Europe and standardises many of the transparency rules for how companies describe and deal with their personal data processing.

It is important to realise that for the purposes of protecting your personal data the GFSC is not a ‘normal’ commercial Gibraltar company. While in common with many other commercial companies we have a CEO, we are established as a statutory body

under the Financial Services Commission Act 2007 and our function is to perform as a public interest regulator. In our case this is the regulation of financial services in Gibraltar. GDPR does not apply to public interest regulators in the same way as it applies to normal commercial companies which may benefit commercially from interactions with you and your personal data. Specifically, Article 6 of GDPR *(Lawfulness of Processing)* states that in the absence of consent from a data subject, data processing will still be lawful if (Art 6(1)(e)):

"…processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

To the greatest extent possible, the GFSC will follow the obligations imposed by the GDPR unless we consider that compliance with any of its provisions would be likely to materially prejudice the proper discharge of our functions or purposes.

DATA CONTROLLER

The Gibraltar Financial Services Commission is the data controller and is responsible for your personal data (collectively referred to as "Commission", "GFSC", "we", "us" or "our" in this privacy policy notice).

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to our privacy policy. The DPO will communicate the decision of whether or not the GFSC will accede to any information request you make (See Section 9 YOUR LEGAL RIGHTS). Therefore, if you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the DPO using the details set out below:

CONTACT DETAILS

Alan Pereira

Gibraltar Financial Services Commission

PO Box 940,

Suite 3, Ground Floor,

Atlantic Suites,

Europort Avenue,

Gibraltar

Email address: apereira@gfsc.gi

You have a legal right to make a complaint at any time to the Gibraltar Regulatory Authority (GRA), which is the statutory Gibraltar supervisory authority responsible for data protection issues in Gibraltar. We would, however, appreciate the chance to deal with your concerns before you approach the GRA, therefore please contact us in the first instance. See also Section 9 YOUR LEGAL RIGHTS of this Privacy Policy.

2. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual person from which that person can be identified. It does not include data where the identity has been removed (anonymous data). Nor does it include data about firms or other legal persons unless it is combined with personal data. If that happens, we always treat the combined data as personal data.

We may collect, use, store, process and transfer different kinds of personal data about you which we have grouped together as follows:

Identity Data includes first name, any pre-marital name, last name, username or similar identifier, marital status, title, date of birth, gender and nationality. It may also include passport or identity card details.

Contact Data includes addresses, email addresses and telephone numbers and any stated communication preferences.

We never collect any Special Categories of Personal Data about you. This includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data.

3. HOW YOUR PERSONAL DATA IS COLLECTED

We use different methods to collect personal data from and about you including the following:

Direct interaction with you

You may give us your Identity, Contact, Financial and other data by filling in forms or by communicating with us by post, telephone, email or otherwise. This includes personal data you provide when you (or a company or other legal person associated with you):

- apply to us or pay for a service (such as a licence or authorisation);
- request information;
- provide feedback or reply to a consultation.

4. HOW WE USE YOUR PERSONAL DATA

We only use your personal data when the law allows us to. Most commonly, we will use your personal data where we need to assess a matter involving a licence, authorisation or financial activity. An example of this is to test that persons who exercise control or significant influence over the operations of a regulated financial firm are fit and proper as well as ensure that they have the correct training and competency to conduct that activity.

Generally, and unlike normal Gibraltar companies, we do not rely on your consent as the lawful basis for processing your personal data. This is because we have a legitimate interest in processing your personal data where it is necessary to comply with a statutory, legal or regulatory obligation, or legitimate request from another public interest regulator.

Please contact us if you need details about any specific legitimate interest we are relying on to process your personal data.

CHANGE OF PURPOSE

We will only ever use your personal data for the purposes we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for a new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal or other basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. DISCLOSURE OF YOUR PERSONAL DATA

We may decide or be required to share your personal data with External Third Parties as set out in the Glossary.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. If we contract with a service provider (such as a law firm, a firm of expert investigators or skilled-persons) we will likewise ensure that that party uses your personal data only for the purposes of the service being provided and only permit them to process personal data for specified purposes and in accordance with our instructions.

The definition of personal data and the principles we abide by in ensuring the confidentiality of a Whistleblower's identity are governed by the same rules further to which we acquire and process personal data in the normal course of our work. These are fully set out in our Privacy Policy here. However, in summary we will:

1. Ensure confidentiality of the information received and protect the identity of a Whistleblower.

2. Apply the principle of data minimisation by only processing personal data, where adequate, relevant and necessary, for a particular case or matter reported to us.
3. Ensure when responding to any right of access or other request to our Data Protection Officer that personal data in respect of a Whistleblower is not revealed.

6. INTERNATIONAL TRANSFERS

We only ever transfer your personal data in accordance with our IT security policies and applicable international standards.

Only in certain limited circumstances will we transfer your personal data outside the European Economic Area (EEA).

These circumstances include:

- the GFSC receiving a valid request for information from a public service regulator or similar relevant entity outside the EEA. We will ensure that a valid request will include at least a similar level of personal data protection as provided within the EEA.
- the GFSC provide your data to an external third-party based outside the EEA. Similarly, we will ensure your personal data receives at least the same level of protection it has in Europe.

Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield. This requires providers in the US to give similar protection to personal data shared between the Europe and the US.

Please contact us if you wish to have further information on the specific mechanism used by us when transferring your personal data outside of the EEA.

7. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from accidental loss, being used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and external third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have procedures in place to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any regulatory, legal, accounting, or reporting obligations or requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from its unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We operate no fixed retention periods for personal data retention.

In some circumstances, you can ask us to delete your data, please see Request Erasure below for further information. The DPO, with reference to the relevant legislation, is responsible for communicating the result of your request to you.

In some circumstances we may anonymise your personal data (for example, by deleting information such as your name, so that this Identity Data can no longer be

associated with you) for research or statistical purposes in which case we may use this information indefinitely without notice to you.

9. YOUR LEGAL RIGHTS

You have a number of rights under data protection laws in relation to the personal data we hold about you, such as the right to request access or corrections or even erasure of your personal data.

While you do have these rights, they will not always be granted in the context of our standing as a public interest regulator (of the Gibraltar financial sector). The decision in respect of such requests will be communicated by our DPO following receipt of a request in writing.

Please visit the GDPR regulation page to find out more about these rights:

- Request access to your personal data
- Request correction of your personal data
- Request erasure of your personal data
- Object to processing of your personal data
- Request restriction of processing your personal data
- Request transfer of your personal data

Please note that as we legally process personal data without your written consent there is no right for you to withdraw that consent.

If you wish to exercise any of the rights set out above, please Contact us

Upon receipt of a written request and subject to being able to prove your identity, the DPO will confirm whether or not we hold personal data about you and if so, what this data is. This data may be provided to you in a readily understood format though note that it may also be redacted.

TIME LIMIT TO RESPOND

We try to respond to all legitimate requests within one calendar month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

RIGHT TO COMPLAIN

You have the right to complain in respect of any of these issues to the Gibraltar Data Protection Commissioner if you think that we have not properly complied with any of the above requirements:

The Gibraltar Data Protection Commissioner

Gibraltar Regulatory Authority

Suite 811, Europort

Gibraltar

Tel +350 200 74636

Fax +350 200 72166

E-Mail info@gra.gi

10. GLOSSARY

LAWFUL BASIS

Legitimate Interest means the requirement upon us (or those of a relevant third party) to conduct and manage our activities to enable us process your personal data where it is necessary to fulfil our statutory, legal and regulatory goals while ensuring the best and most secure data experience.

EXTERNAL THIRD PARTIES

Service providers acting as data processors based either inside or outside the EEA who provide various services to us. An example would be a supplier of external IT, data processing or software application services.

Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based inside or outside the EEA who provide consultancy, banking, legal, insurance and accounting services. Examples are outsourcing investigations to third parties or obtaining advice from a legal firm.

Other Gibraltar and non-Gibraltar regulators or public bodies both inside or outside the EEA acting in a public interest and acting as processors or joint controllers based within and without Gibraltar who require reporting of processing activities in certain circumstances. We may share your personal data via a number of gateways, including the various Multilateral Memorandum of Understanding (MMoU) and Memorandum of Understanding (MoU) routes to which we are a signatory. Examples of the former are our memberships of the International Association of Insurance Supervisors (IAIS) and the International Organisation of Securities Commissions (IOSCO); and examples of the latter are our MoU's with the Malta Financial Services Authority and the Royal Gibraltar Police. A list of the GFSC's current bilateral and multilateral commitments to share information in this way may be viewed here: http://www.gfsc.gi/international/mmou. This sharing can come about either at our request or the request of another signatory or other regulatory party; and compliance may be either optional or obligatory on us. However, the sharing comes about we will never sell or trade your data, and will only ever share your personal data subject to a data protection standard which is at least the equivalent of the EU standard.

YOUR LEGAL RIGHTS

These are set out in Section 9

END of PRIVACY POLICY