Privacy notice for Global Health and Accident Insurance Limited

Global Health and Accident Insurance Limited are committed to protecting the privacy and security of your personal information.

We are responsible for deciding how we hold and use personal information. We are required under data protection legislation to notify you of the information contained in this privacy notice.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with the relevant data protection laws. This means that the personal information we hold about you must be:

1. **Used lawfully, fairly and in a transparent way.**
2. **Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.**
3. **Relevant to the purposes we have told you about and limited only to those purposes.**
4. **Accurate and kept up to date.**
5. **Kept only as long as necessary for the purposes we have told you about.**
6. **Kept securely.**

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are 'special categories' of more sensitive personal data that require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Former names.
- Date of birth.
- Place of birth.
- Nationality.
- Passport number and country of issue.
- Tax Identification Number.
- Tax Residency.
- Occupation, name of employer, nature of employment.
- Business address.
- Whether you have held a public position or office.
- Source of funds, source of wealth information.
- Copy of driving license or ID card, where applicable.

We may also collect, store and use the following 'special categories' of more sensitive personal information:

- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We typically collect personal information about you through our client take-on process or application forms either directly from you as you complete our mandatory forms, from a third party advisor (such as your lawyer), from publicly available sources (such as the Guernsey Registry, Companies House or a subscription identification verification database.

We may collect additional personal information in the course of our business relationship with you.

How we will use information about you

We will only ever use your personal information when the law permits or compels us. Most commonly, we will use your personal information in the following circumstances:

1. **To verify your identity and protect against fraud and to fulfil our Anti-Money Laundering and Combating the Financing of Terrorism obligations**
2. **Where it is necessary to perform the contract we have entered into with you**
3. **Where it is necessary to comply with a legal obligation**
4. **Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.**

We may also use your personal information in the following situations, which are likely to be rare:

1. **Where we need to protect your interests (or someone else's interests).**
2. **Where it is needed in the public interest (or for official purposes).**
3. **If required to verify a claims under the policy**

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform the contracted services and to enable us to comply with our legal obligations. Examples of the situations in which we will process your personal information are listed below. We have indicated the purpose (or purposes) for which we are processing (or will process) your personal information, as well as indicating the categories of data involved.

During the course of our business relationship, we may:

- **Where we are compelled, or permitted to do so by law, disclose your personal information to any law enforcement agency or regulatory body.**
- **Open, maintain or administer bank accounts.**
- **Consult with legal counsel for the purposes of obtaining legal advice.**
- **Assist in verification of a claims**

Some of the above grounds for processing will overlap and there may be several which require our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to provide the services you have required, as this may prevent us from complying with our legal obligations such as to fulfil our Anti-Money Laundering and Combating the Financing of Terrorism obligations.

Change of purpose

We will only use your personal information for the purposes necessary for which 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 we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

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

How we use particularly sensitive personal information

'Special categories' of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. **In limited circumstances, but only with your explicit written consent.**
2. **Where we need to carry out our legal obligations and in line with our Privacy Policy.**

Less commonly, we may process this type of information where it is required in relation to legal claims or where it is needed to protect your interests (or another person's interests) and you are incapable of giving your consent, or where you have already made the information public.

High risk data use

We are required by law to determine whether the use of your personal data carries a high risk of 'physical, material or non-material damage' to you. We have put in place procedures to assess whether the use of your personal data is considered to be high-risk. In the unlikely event that the use of your personal data is considered to be 'high risk' our Data Protection Officer shall take certain measures to address such risk and any suspected data breach shall be notified to you immediately where we are required by law to do so.

Our obligations as an employer

Each and every one of our employees or third party administrator (Goldencare SA) is responsible for maintaining the confidentiality of all personal information to which they have access. As an express condition of their contracts of employment, our employees must assume and maintain obligations of confidentiality which endure beyond the cessation of employment.

All employees are required to undertake mandatory data protection training on a regular basis which reinforces their responsibilities and obligations in maintaining the privacy and confidentiality of your personal information.

Do we need your consent?

We do not need your consent if we use special categories of your personal information to carry out our legal obligations. In limited circumstances, we may approach you (or your representative) for written consent to allow us to process certain particularly sensitive data. If we do so, we will provide full details of the information that we would like and the reason we need it, so that you may consider if you wish to consent.

Information about unlawful activity

We may only process information relating to unlawful activity where the law allows us to do so. We will use financial crime or other background check agencies to screen you as part of the client take-on process, or we may be notified of such information directly by you in the course of our business relationship. We will use information about unlawful activity to fulfil our Anti-Money Laundering and Combating the Financing of Terrorism obligations.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside of Guernsey or the European Union (EU). If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We may share your personal information with third parties, where required to do so by law or where it is necessary to provide the services you have requested from us.

Which third-party service providers process my personal information?

'Third parties' includes third-party service providers (including contractors and designated agents) and other offices. The following are examples of the types of activities that may be carried out by third-party service providers:

- Archive data storage.
- Legal advice.
- Claims and premium administration
- Banking and brokerage services.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party

service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Transferring information outside Guernsey and the EU

We may transfer the personal information we collect about you to other countries in order to perform our contract with you. There may not be an adequacy decision by the European Commission in respect of those countries. This means that the countries to which we transfer your data are not deemed to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive an adequate level of protection, we have put in place a Data Processing Agreement, to be used in conjunction with EU Standard Contract Clauses, to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU, UK and Guernsey laws on data protection. If you require further information about this protective measure, you can request it from our Data Protection Officer.

Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure. Details of these measures may be obtained from our Data Protection Officer.

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

Data retention

How long will you use my information for?

We will retain your personal information for as long as necessary to fulfil the purposes we collected it for. The length of time we retain your personal information depends on:

- the purposes for which we process your personal data.
- any legal or regulatory requirement we may have to meet.

For example, we must be able to respond to any concerns you may have, even if you are no longer a client. We have retention policies in place that govern the destruction of personal information.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once your business relationship with us has ended we will retain and securely destroy your personal information in accordance with our data retention policy and applicable laws and regulations.

Your duty to inform us of changes

We are committed to retaining the accuracy of your personal information for as long as it is being used for the purposes set out in the policy, and provided that you keep us up to date. Prompt notification of any changes, such as your address, email address or telephone number, will help us provide you with the best possible service. Should you discover, upon review of your personal information, that amendments are required, please advise us immediately. We will make our best efforts to advise others of any important amendments to your personal information that we may have released to them.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a 'data subject access request'). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground.
- **Request the restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our Data Protection Officer in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the requests that we deem unfounded or excessive.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who is not entitled to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this Privacy Notice

This Notice does not form part of any contract to provide services.

We reserve the right to update this Privacy Notice at any time, and will notify you accordingly.

Supervisory Authority

You have the right to make a complaint at any time to Guernsey's supervisory authority for data protection issues:

The Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade, St Peter Port
Guernsey
GY1 2LQ

Telephone: +44 1481 742074
Email: enquiries@dataci.org

Data Protection Officer

We have appointed a Data Protection Officer to oversee compliance with this Privacy Notice. If you have any questions about this Privacy Notice or how we handle your personal information, please contact the following:

Data Protection Officer
Artex Risk Solutions (Guernsey) Limited
PO Box 230
Heritage Hall
Le Marchant Street
St Peter Port
Guernsey
GY1 4JH

Telephone: +44 1481 737100