Privacy Policy

Acapella Syndicate 2014, managed by Ironshore International's Pembroke Managing Agency Limited, is well aware that our relationship with you is based upon trust. That trust is premised, in part, on our promise to you that we will protect your personal data and use it only in the ways described in this Privacy Policy.

This Privacy Policy will provide you with information on:

- Who We Are
- What personal data Ironshore collects from you or about you from third parties
- How Ironshore uses that personal data and the lawful basis to do so
- Who else may access your personal data
- Where your personal data may be stored or transferred
- How we secure your data
- How long we keep your data
- The rights you may have to learn more about the personal data we process.

Insurance can be confusing, but we don't want this policy to be as well. Let's start with some basics. Personal Data is defined as it is in the EU's General Data Protection Regulation. In essence, it means data that directly or indirectly identifies you. To assist your understanding of how personal data may flow through the insurance process, we set out at **Annex 1** a diagram of the various stages of insurance and an overview of who may need your personal data to perform the relevant obligations connected to your relationship with us.

This Privacy Policy covers our interactions with you, but does not cover your visits to the Ironshore.com or Acapella-underwriting.co.uk website. For information about how we collect and use your personal data from your use of our website and the links contained therein, please see our Website privacy notice. For the avoidance of doubt, the website privacy notice supplements this Privacy Policy and is not intended to override the Privacy Policy.

This version of the Privacy Policy is effective as of 25 May 2018. Any future changes to the Privacy Policy will be posted here. Historic versions can be obtained by contacting us at dataprotection@ironshore.com.

Questions about this Privacy Policy and how we process your data may be sent to

Data Protection Officer
Ironshore International Ltd
8 Fenchurch Place
London
EC3M 4AJ
dataprotection@ironshore.com

WHO WE ARE

Ironshore is made up of different legal entities, details of which can be found on our website. This Privacy Policy is issued on behalf of Ironshore, its parent company, Liberty Mutual Group Inc., and all of the Ironshore and Liberty affiliates and subsidiaries including Acappella Syndicate 2014 (now collectively referred to as "Ironshore Group"). When we mention "Ironshore" "we", "us" or "our" in this Privacy Policy, we are referring to the relevant company in the Ironshore Group responsible for processing your data.

When a company processes your personal data, it is either a "controller" or a "processor." In different circumstances, Ironshore may be either. Let's look at a few examples:

If you took out the insurance policy with us yourself:
We will be the data controller if you took out the policy directly with us. Contact information for our Data Protection Officer is set out below

Data Protection Officer
Ironshore International Ltd.
8 Fenchurch Place
London
EC3M 4AJ
dataprotection@ironshore.com

If you are making a claim in relation to an Ironshore policy:
We will be the data controller if the claim relates to a policy with us. Contact information for our Data Protection Officer is set out below.

Data Protection Officer
Ironshore International Ltd.
8 Fenchurch Place
London
EC3M 4AJ
dataprotection@ironshore.com

If you took out the insurance policy with a broker / other intermediary:
If you purchased a policy with a broker or other intermediary, the broker / intermediary will be the initial data controller and their data protection contact can advise of the identities of the entities with whom they share your personal data.

If you are not a policyholder or an insured, or not sure if we hold personal data about you:
You should contact the organisation that collected your personal data who, in turn, should provide you with details of the entities with whom they share your personal data.

WHAT PERSONAL DATA IRONSHORE COLLECTS FROM YOU OR ABOUT YOUR FROM THIRD PARTIES

We collect personal data about you in two main ways: directly from you and from third parties.

- Direct interactions. You may give us certain data including your identity and contact data and other personal data required for the purpose of entering into a policy with us.

- Third parties or publicly available sources. We may receive personal data about you from various third parties such as your employer, other insurers or brokers who you have communicated with in relation to your policy, anti-fraud databases, sanctions lists, court judgments and other databases, government agencies, open electoral register or in the event of a claim, third parties including the other party to the claim (claimant / defendant), witnesses, experts (including, where applicable, medical experts), loss adjustors, solicitors and claim handlers. We may also collect data about you from third parties who take out a policy with us and are required to provide your information, e.g., where you will be a named beneficiary of the policy or where a family member has taken out a policy which requires personal information about you.

The sources where we collect your personal data will depend on your particular circumstances.

For us to provide insurance quotes, policies, process any claims you may have in connection with one of our policies (whether it is between you and us, or a third party and us but under which you have a claim) and to deal with any concerns, we will need to collect and process certain personal data about you.
The types of personal data we may have to process will depend on the nature of your policy, claim and / or complaint may include the information such as that defined below.

Type of Personal Data and Details About It

1. **Identity and where applicable, identification data**
   Including: given names, title, gender, age, nationality, date and place of birth, marital status, employer, job title, employment history, family details (including information about their relationship to you), identification numbers issued by government bodies or agencies, tax identification number.

2. **Contact Data**
   Including: email address, telephone number, address

3. **Financial Data**
   Including: bank account or payment card details, income or other financial information

4. **Risk Data**
   Including: information about you which we need to collect in order to assess the risk to be (re)insured and to provide a suitable quote. In relation to certain lines of business such as personal accident, this may include data relating to your health or other special categories of personal data. It may also include information about criminal convictions.

5. **Policy Data**
   Including: information about the quotes you receive and policies you take out

6. **Credit and anti-fraud data**
   Including: data about sanctions, criminal offences and information received from anti-fraud databases relating to you (including credit history, where applicable)

7. **Previous and current claim data**
   Including: information about previous and current claims (such as unrelated insurance cover with us). This may include data relating to your health, criminal convictions, third party reports or special categories of personal data.

8. **Special categories of personal data**
   Given our business, we consider it will only be necessary to process this information in limited circumstances such as to process a personal accident claim where we may need information about your health. We may also need information about your criminal convictions in order to process any claim or complaint.

HOW IRONSHORE USES THAT PERSONAL DATA AND THE LAWFUL BASIS TO DO SO

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- 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.
- Where we need to comply with a legal or regulatory obligation.
- If you have a policy with us or otherwise benefit from a policy which a third party (such as an employer or family member) has entered into with us, where we need to perform the contract we are about to enter into or have entered into with you or the relevant third party.

It may be necessary for us to process your personal data such as policy data and claims data using automated analysis and human discretion to ensure premiums properly reflect the relevant underlying risks. This is may also be used to ensure our claims process are fully effective. We do not use any special categories of sensitive personal data such as information about your health or criminal convictions for profiling purposes.

Below you will find a description of the ways we plan to use your personal data, and the legal basis we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

Overview of Legal Basis Relied on by Us to Process Your Personal Data

The information below identifies the different purposes, or types of activities for which we may collect personal data, the type of data collected and the lawful basis for doing so.

1. Quotation Inception
   1.1. Setting you up as a client, including fraud, credit and anti-money laundering and sanctions checks

   Type of Data:
   - Identification Data
   - Contact Data
   - Financial Data
   - Credit and anti-fraud data

   Lawful basis for processing including basis of legitimate interest
   - Performance of a contract with you
   - Compliance with a legal obligation (i.e., to ensure we do not provide cover in breach of applicable laws and regulations)
   - Legitimate interests (i.e., to ensure you are within our acceptable risk profile)

   1.2. Evaluating the risks to be covered and matching those risks to the appropriate policy and premium

   Type of Data:
   - Identification data
   - Risk data
   - Policy data
   - Previous claims data
   - Credit and anti-fraud data

   Lawful basis for processing including basis of legitimate interest
   - Performance of a contract with you
   - Legitimate interests (i.e., to determine the likely risk profile and appropriate insurance product and premium)
   - Compliance with a legal obligation (i.e., to ensure we do not provide cover in breach of applicable laws and regulations)

2. Policy Administration
   2.1. Collecting or refunding premium to an individual

   Type of Data:
   - Identification data
   - Contact data
   - Financial data

   Lawful basis for processing including basis of legitimate interest
   - Performance of a contract with you
   - Legitimate interests (e.g., to recover debts due to us)

2.2. General client care, including communicating with you in relation to administration and requested changes to your policy. We may also send you updates regarding any policy you have taken out with us or under which you are a beneficiary

Type of Data:

- Identification data
- Contact data
- Policy data
- Risk details
- Current and previous claim data

Lawful basis for processing including basis of legitimate interest

- Performance of a contract with you
- Legitimate interest (i.e., so that we can correspond effectively with our insureds /policy holders, beneficiaries in relation to policies or those who have made claims pursuant to or connected to a policy entered into with us. This information will also facilitate the processing and payment of claims (see below)

3. Claims Processing

3.1. Managing all aspects of claims handling and processing, including fraud, credit and AML and sanctions checks

Type of Data: Identification data

- Contact data
- Risk data
- Financial data
- Policy data
- Current and previous claim data
- Credit and anti-fraud data

See section below concerning instances where we might need special categories of sensitive personal data including information about your health and criminal convictions

Lawful basis for processing including basis of legitimate interest

- Performance of a contract with you
- Legitimate interests (e.g., to recover debts due to us)

3.2. General client care, including communicating with you in relation to administration and requested changes to your policy. We may also send you updates regarding any policy you have taken out with us or under which you are a beneficiary

Type of Data:

- Identification data
- Contact data
- Policy data
- Risk details
- Current and previous claim data

Lawful basis for processing including basis of legitimate interest

- Performance of a contract with you
- Legitimate interests (i.e., to assess the veracity and quantum of claim(s))
- Compliance with a legal obligation (i.e., to ensure we do not pay a claim in breach of applicable laws and regulations)

3.3. Defending or making legal claims

Type of Data:

- Identification data
- Contact data
- Risk data
- Financial data
- Policy data
- Current and previous claim data
- Credit and anti-fraud data

See section below concerning instances where we might need special categories of sensitive personal data including information about your health and criminal convictions

Lawful basis for processing including basis of legitimate interest

- Performance of a contract with you
- Legitimate interests (i.e., to defend or make necessary legal claims)
- Compliance with a legal obligation (i.e., to ensure we comply with all applicable rules and laws)

3.4. Investigating and assisting where applicable in the prosecution of fraud

Type of Data:

- Identification data
- Contact data
- Risk data
- Financial data
- Policy data
- Current and previous claim data
- Credit and anti-fraud data

See section below concerning instances where we might need special categories of sensitive personal data including information about your health and criminal convictions.

Lawful basis for processing including basis of legitimate interest

- Performance of a contract with you
- Legitimate interests (i.e., to assist with the prevention or detection of fraud)
- Compliance with a legal obligation (i.e., to ensure we comply with all applicable rules and laws)

4. Renewals

4.1. Where you have taken out a policy as an individual, contacting you in order to renew the policy

Type of Data: Identification data

- Identification data
- Contact data
- Policy data

Lawful basis for processing including basis of legitimate interest

- Performance of a contract with you
- Legitimate interests (i.e., to correspond with insured / policy holder / beneficiary to facilitate the placing of applicable cover under insurance policies

5. Other Uses

5.1. Transfers of books of business, company sales and reorganisations

Type of Data: Identification data

- Contact data
- Risk data
- Financial data
- Policy data
- Current and previous current claims data
- Credit and anti-fraud data

See section below concerning instances where we might need special categories of sensitive personal data including information about your health and criminal convictions

Lawful basis for processing including basis of legitimate interest

- Legitimate interests (i.e., to structure our business appropriately)
- Compliance with a legal obligation

5.2. Complying with our Legal Obligations

Type of Data: Identification data

- Contact data
- Risk data
- Financial data
- Policy data
- Current and previous current claims data
- Credit and anti-fraud data

See section below concerning instances where we might need special categories of sensitive personal data including information about your health and criminal convictions

Lawful basis for processing including basis of legitimate interest

- Compliance with a legal obligation

5.3. General risk modelling and underwriting

Type of Data: Identification data

- Identity / identification data
- Contact data
- Risk data
- Financial data
- Policy data
- Current and previous claims data
- Credit and anti-fraud data

See section below concerning instances where we might need special categories of sensitive personal data including information about your health and criminal convictions

Lawful basis for processing including basis of legitimate interest

- Legitimate interests (i.e., to build risk models that allow for the acceptance of risk with appropriate premiums)

Special Categories of Data: As we have indicated in the sections above in order to process certain polices and / or claims connected to those policies, it may be necessary for us to collect and process certain special categories of data. However, given the limited likelihood of us needing to obtain this information from you, where we do need this information we will write to you to obtain your consent for processing this information. You may withdraw your consent to such processing at any time. However, if you withdraw your consent this may impact our ability to provide you with insurance cover or pay claims.

Change of Purpose: We will only use your personal data for the purposes 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 you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact our Data Protection Officer.

If we need to use your personal data 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 data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

WHO ELSE MAY HAVE ACCESS TO YOUR PERSONAL DATA

We may need to share your personal data information with third parties. For example, we may need to share your personal data to provide you with the insurance under your policy or to pay or otherwise investigate any claim arising from a policy entered into with us.

We share your personal data within the Ironshore Group and where necessary to perform essential business functions, we share your personal data with our authorised external third parties. For example, to process claims effectively and to carry out necessary business functions, a company called Genpact provides functional support to Ironshore. Another example is in data storage and processing. Ironshore, like many companies, uses cloud service providers ("CSP") to provide functional IT support. This includes the storage of personal data you provide to us. Any personal data provided to a third party is used solely for Ironshore's necessary business functions.

We may also transfer data to appropriate third parties as required by applicable laws, rules and regulations, in response to a lawful request from governmental authorities, or to comply with legal process.

We will get your express opt-in consent before we share your personal data with any company outside the Ironshore Group for marketing purposes.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

WHERE YOUR PERSONAL DATA MAY BE STORED OR TRANSFERRED

We share your personal data within the Ironshore Group and our authorised external third parties. The Ironshore Group and these third parties are located across the world. Some of these countries may be subject to additional or different data protection requirements. Where this is the case, we will take appropriate measures to protect your personal information in accordance with this notice and all applicable data privacy laws.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.
- We may transfer data to them if they are part of the U.S. Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US.
- They have EU approved binding corporate rules or other EU approved certifications.

Please contact us if you want further information on the specific mechanism we use when transferring your personal data out of the EEA.

HOW WE SECURE YOUR DATA

Ironshore maintains physical, electronic, and procedural safeguards that comply with applicable regulations to guard your personal data. We limit access to your personal data to those employees, agents, contractors and other third parties who have a business-need to-know. They will only process your personal data on our instructions. We have put in place procedures to deal with any suspected unauthorized access or loss of personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

HOW LONG WE KEEP YOUR DATA

By law we have to keep basic information about our customers (including Contact, Identity / Identification and Financial Data) for a required period of time even, in some circumstances, after your relationship with Ironshore has ended. In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you. Please contact us if you require specific information about the retention period of your personal data.

YOUR LEGAL RIGHTS

Under certain conditions, you may have the right to require us to:

- provide you with further details on the use we make of your personal data;
- provide you with a copy of the personal data you have provided to us;
- update inaccuracies in the personal data we hold;
- delete personal data we no longer have a lawful ground to use;
- where processing is based on consent, to withdraw your consent so that we stop that particular processing;
- object to any processing of your personal data that we do based on the legitimate interests ground unless our reasons for undertaking that processing outweigh any prejudice to your data protection rights; and
- restrict how we use your personal data whilst a complaint is being investigated.

In certain circumstances, we may need to restrict the above rights in order to safeguard the public interest (e.g. the prevention or detection of crime) and our interests (e.g. the maintenance of legal privilege).

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that your personal data is not disclosed to any other person. We may also ask you for further information to clarify your request.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month. In this case, we will notify you and keep you updated.

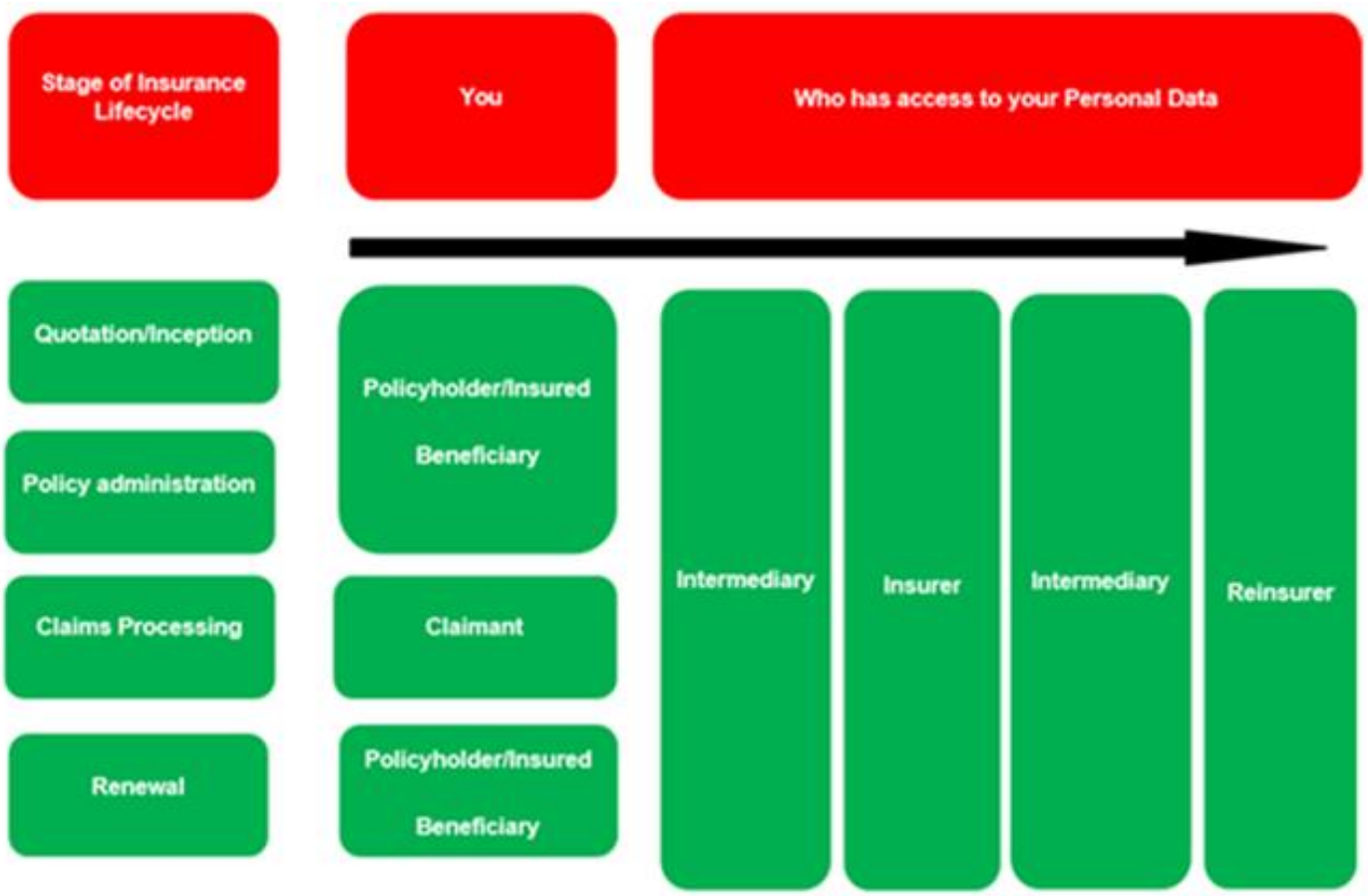
You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

If you wish to exercise any of the rights, please contact our Data Protection Officer by submitting the data subject request form found here http://www.ironshore.com/subject-rights-access-form.php.

We have appointed a Data Protection Officer. If you have any questions about this Privacy Policy or our processing activities, please contact the Data Protection Officer at dataprotection@ironshore.com While we would appreciate the opportunity to address your concerns first, you may have the right to make a complaint to the relevant national supervisory authority for data protection issues. If you are a resident of the UK, for example, you can make a complaint at any time to the Information Commissioner's Office (ICO) (www.ico.org.uk).

Annex 1

Flows of Personal Data through the Insurance Lifecycle



Acappella Syndicate 2014
Level 3
8 Fenchurch Place
London, EC3M 4AJ
+44 (0)20 7337 4400
www.acappellaunderwriting.com