Spitfire Corporation Limited
Privacy Policy

16 August 2019

Privacy Policy

When does this policy apply?

This policy sets out the principles that Spitfire Corporation Limited and its related body corporates (Spitfire Group) as defined in the Corporations Act 2001 (Cth) (Spitfire/we/us/our) adopt in the conduct of our business in order to protect your Personal Information. A number of our related body corporates engage in activities under other brands. You can contact the Spitfire Group Privacy Officer to verify the details of the corporate group entity that this policy applies to. You can obtain a copy of this policy by contacting our Privacy Officer whose details are set out below.

Protecting your privacy

Spitfire is committed to providing you with exceptional service, and this includes protecting your privacy and being open and transparent about what we do with your Personal Information. We aim to maintain a safe and secure system of handling your Personal Information, whilst still providing access to your Personal Information when required. For this reason, we aim to ensure that your Personal Information is handled in strict compliance with the Australian Privacy Principles (APPs) which are part of the Privacy Act 1988 (Cth) (Privacy Act).

This Policy

This policy explains what kinds of Personal Information we collect and hold; how and why we collect, hold and use it; and how and to whom we disclose that Personal Information. It also provides details about how you may access and seek correction of the Personal Information that we hold about you, and what you can do if you are not satisfied with how we have dealt with your Personal Information.

What is Personal Information and how do we collect it?

Personal Information is information or an opinion about an individual from which they can be reasonably identified. Depending on the circumstances, we may collect Personal Information from an individual in their capacity as a client, customer, contractor, stakeholder, job applicant, or in some other capacity.

In the course of our business and providing products and services we may collect and hold:

- **Personal Information** - which means information or an opinion about an identified individual or individual who is reasonably identifiable and which includes names, addresses and other contact details; dates of birth; and financial information.
- **Sensitive Information** - including government identifiers (such as TFN), nationality, country of birth, professional memberships, family court orders, and criminal records.

As part of our recruitment processes for employees and contractors, we may collect and hold:

- **Personal Information** including names, addresses and other contact details, dates of birth, financial information, citizenship, employment references, regulatory accreditation, media, directorships, property ownership and driver's licence information.
- **Sensitive Information** including government identifiers (such as TFN), nationality, country of birth, professional memberships, family court orders, and criminal records.

Generally, we will seek consent from you in writing before we collect your sensitive information.

Collection of Personal Information

We only collect Personal Information about you that is necessary for us to carry on our business functions. The information we collect about you depends upon the nature of our dealings with you. Without your Personal Information, we may not be able to process your application or contribution or provide you with the appropriate product and services. Generally, we only collect Personal Information from you, unless it is not reasonable or practical to do so, in which case we may also collect Personal Information about you from third parties.

Information we collect from you

We collect Personal Information from you during your interactions with us, for example if you:

- make an enquiry about our products or services
- phone, email or write to us, or visit our website
- purchase our services or products online
- subscribe to receive information or updates about our services or provide your details for our mailing list
- make an application to invest with us
- or another individual, makes a complaint.

We may collect Personal Information (including sensitive information) based on how you use our website. We use ''cookies" and other data collection methods to collect information on website activity such as the number of visitors, the number of pages viewed and the internet advertisements which bring visitors to our website. This information is collected to analyse and improve our website, marketing campaigns and to record statistics on web traffic.

If you access your account with us online through a secure area of our website, it will collect your Personal Information using cookies. This is designed to track the use of our website and to allow individuals to effectively access their account information. This information is collected for security purposes and to protect the integrity of account details.

Information we collect from others

We will collect Personal Information about you from third parties such as:

- our service providers. For example, when you make an enquiry about our products or services to our service providers who assist us in providing our products or services to you;
- your financial adviser, accountant, agent, or third-party intermediaries and you have agreed for your Personal Information to be shared with us;
- someone that is appointed as your personal representative, attorney or legal representative; and
- third parties to whom you have provided your Personal Information and consented for that information to be shared with us.

However, we will only do so where it is not reasonable and practical to collect the Personal Information from the individual directly.

Collection of Sensitive Information

On rare occasions, we may need to collect information of a more sensitive nature. The following is considered "sensitive information":

- Racial or ethnic origin
- Political opinion
- Political association membership
- Religious beliefs or affiliations
- Philosophical beliefs
- Professional or trade association membership
- Trade union membership
- Sexual orientation or practices
- Criminal records
- Genetic information

We only collect sensitive information if it is:

- reasonably necessary for one or more of our business functions or activities, and we have your consent;
- required by applicable laws or rules; and
- a permitted general situation as defined in the Privacy Act. We may share your sensitive information to other entities in our company group, but only if necessary for us to provide our products or services.

Individual rights

Wherever it is lawful and practicable, we will give you the option of not providing information when dealing with us. However, in most cases, if you do not provide the full and complete information requested we will be unable to provide our products or services to you.

Using your Personal Information

We only use your Personal Information for:

- the reasons we collected it; that is where it is reasonably necessary for one or more of our business functions or activities (the primary purpose);
- a related secondary purpose that would be reasonably expected by you;
- the purposes set out in this policy; and
- an activity or purpose to which you have consented.

We use your Personal Information so we can, amongst others:

- establish and verify your identity;
- provide, manage and administer the provision of our products and services to you;
- provide you with information about financial products and services;
- process a payment, including credit card payment;
- implement investment instructions, process distributions and withdrawal applications;
- report the investment performance of accounts;
- assess your application and eligibility for any financial product or financial service;
- contact you and manage our relationship with you;
- identify and tell you about other products or services that we think may be of interest to you (unless you tell us not to);
- conduct, manage and improve our business and our customers experience (including through the use of data analytics);
- design, price and administer our products and services;
- manage our risks and identify and investigate illegal activity, such as fraud, bribery or corruption;
- comply with our legal and regulatory obligations such as those under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act and AML/CTF Rules) and assist government and law enforcement agencies or regulators; and
- provide or assist you with other services that you may request from time to time.

We may also collect, use and exchange your information in other ways where required by law or permitted by the Privacy Act.

Marketing

We may use your Personal Information to directly offer you products and services that we believe may be of interest and value to you, but we will not do this if you tell us not to. These products and services may be offered by a member of the Spitfire Group or one of its preferred suppliers by various means, including by mail, telephone, email, SMS or through social media or targeted advertising through Spitfire or non-Spitfire websites. When we market products and services to you, we will comply with applicable privacy laws to obtain your consent if required. If you do not want to receive marketing offers from us, you can tell us by emailing us and telling us which list you would like to be removed from at contact@spitfire.io or write to us at GPO Box 4970 Sydney NSW 2000. If we undertake direct marketing we acknowledge that we are bound by the Spam Act 2003 and the Do Not Call Register Act 2006.

Using government identifiers

If we collect government identifiers, such as your tax file number, we do not use or disclose this information other than required by law.

Disclosure of Personal Information

The reasons for disclosing your Personal Information and the parties to whom we might disclose it will be reasonably apparent to you when we collect your information. Our disclosure of your Personal Information will only be in connection with our business activities or where you have given consent. Where Personal Information is disclosed to any third party we will take reasonable steps to ensure that the person receiving your Personal Information keeps it confidential and does not misuse it or improperly disclose it to any other person.
Personal Information may be shared between different entities within the Spitfire Group but where this occurs the principles contained in this policy will continue to apply to it.

We may disclose your Personal Information without your consent if:

- we are required to do so by law or court order;
- a permitted general situation as defined in the Privacy Act exists; and
- disclosure is reasonably necessary for a law enforcement related activity.

We may disclose your Personal Information to the following parties:

- our product and service providers who provide, manage or administer our products or services on our behalf;
- our product and service providers who assist us to provide, manage or administer our products or services to you;
- consultants and contractors and their sub-contractors who provide services to us;
- our representatives, associates, joint venture partners, partners, agents;
- our professional advisers;
- those to whom we outsource certain functions, for example, postage, marketing, printing, accounting, administration, debt recovery and IT support;
- referees provided by you to us;
- insurers and re-insurers;
- auditors;
- any person considering acquiring an interest in our business or assets;
- any organisation providing verification of your identity (including information you have told us as part of AML/CTF Know Your Customer checks), or bank account, credit card or other payment information;
- claims-related providers, such as assessors and investigators, who help us with claims;
- financial institutions, for example so that we can process a claim for mistaken payment;
- government and law enforcement agencies or regulators;
- any industry body, tribunal, or court;
- entities established to help identify illegal activities and prevent fraud;
- any person where we are required by law to do so; and
- any person or organisation where you have given your consent.

We will not sell your Personal Information to other organisations.

Disclosure of your Personal Information to overseas recipients

We may disclose your Personal Information to an overseas organisation in the course of providing our products or services to you, for example if any of the above named parties are located overseas, or directly to our agents in an overseas location, or when storing information with a “cloud service provider” which stores data outside of Australia. Where we do this, we make sure as far as reasonably possible and where practicable that:

- we have your consent (which may be implied);
- we have satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime;
- appropriate data handling and security arrangements are in place;
- we form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
- we are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

Please note that some of these overseas recipients may not operate in countries which have a similar privacy regime to Australia.

Storage and security of Personal Information

We store Personal Information in a variety of formats including, but not limited to:

- electronic databases;
- cloud based databases and storage facilities;
- hard copy files;
- personal devices, including laptop computers;
- third party storage providers such as cloud storage facilities; and
- paper based files.

We take all reasonable steps to protect the Personal Information we hold from misuse, loss, unauthorised access, modification or disclosure.

These steps include, but are not limited to:

- restricting access and user privilege of information by staff depending on their role and responsibilities;
- ensuring staff do not share personal passwords;
- ensuring hard copy files are stored in lockable filing cabinets in lockable rooms. Staff access is subject to user privilege;
- ensuring access to our premises is secured at all times;
- ensuring our IT and cyber security systems, policies and procedures are implemented and up to date;
- ensuring staff comply with internal policies and procedures when handling the information;
- undertaking due diligence with respect to third party

service providers who may have access to Personal Information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime; and

- the destruction, deletion or de-identification of Personal Information we hold that is no longer needed, or required to be retained by any other laws.

Our public website may contain links to other third-party websites outside of the Spitfire Group. We are not responsible for the information stored, accessed, used or disclosed on such websites and we cannot comment on their privacy policies.

Responding to data breaches

We will take appropriate, prompt action if we have reasonable grounds to believe that a data breach may have, or is, suspected to have occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC). If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

The quality of Personal Information

We take all reasonable steps to ensure the Personal Information we hold, use and disclose is accurate, complete and up-to-date, including at the time of using or disclosing the information.
If we become aware that the Personal Information is incorrect or out of date, we will take reasonable steps to rectify the incorrect or out of date information.

How do you access your information?

You may ask us what Personal Information we hold about you, and you may make a request to access to this information at any time. You may make a request by us by contacting our Privacy Officer (see below contact details). We may ask you to complete a PERSONAL INFORMATION REQUEST FORM and will process your request within a reasonable time and try to make this information available within 30 days of your request. Before we give you the requested information we will need to confirm your identity.

We generally will not charge you a fee in respect of such access but reasonable administrative costs may be charged in some circumstances. If there is an access charge, we will give you an estimate first and ask you to confirm that you would like us to proceed, and if you would like us to proceed we will require payment up front. Generally, the access charge is based on an hourly rate plus any other reasonable costs incurred by us such photocopying and postage. We do not need to provide access to your information in several circumstances; for example, the information is commercially sensitive, the request is frivolous or would unreasonably interfere with another person's privacy or be in breach of the law, or, where to provide access would pose a threat to health or public safety. If we refuse you access we will advise you of our reasons for doing so.

How do you correct or update your information?

You may ask us at any time to correct the information we hold about you or that we have provided to others us by contacting our PRIVACY OFFICER (see below contact details). We will process your request within a reasonable time and try to correct the information within 30 days. If it looks like it will take longer, we will let you know the reason for the delay and try to agree to an extended timeframe with you. If we are able to correct your information because it is indeed inaccurate, we will inform you when it is corrected.

If we disagree with you that the information is inaccurate and should be corrected, we will inform you in writing of our reasons. You may request that we attach a statement to that relevant information noting that you consider it is inaccurate misleading, incomplete, irrelevant or out-of-date. We will take reasonable steps to comply with such a request.

How do we destroy or de-identify your information?

If we no longer require Personal Information we hold, we will destroy or de-identify the information. If held in hard copy form, the information is destroyed through a secure process of document destruction. If held in electronic form, steps are taken to irretrievably destroy the information or put it 'beyond use'.

Complaints

If you are not happy in respect of how we have dealt with your Personal Information or in gaining access to it, please contact our Privacy Officer to discuss your concerns (see below contact details). We will respond to the complaint within a reasonable time (usually no longer than 30 days) and we may seek further information in order to provide a full and complete response. If we do not resolve your complaint to your satisfaction or we are unable to resolve your complaint you have the right to refer the matter the Office of the Federal Privacy Commissioner – Privacy Hotline on 1300 363 992 or visit their website at www.oaic.gov.au or write to GPO Box 5218 Sydney NSW 2001. A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

How to Contact Us

Privacy Officer

- Email: contact@spitfire.io
- Phone: 1300 710 866
- Address: GPO Box 4970 Sydney NSW 2001

If practical, you can contact us anonymously (that is, without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

Changes to our privacy and information handling practices

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website (www.spitfire.io) regularly for any changes.

1300 710 866

contact@spitfire.io or visit us online at www.spitfire.io

GPO Box 4970 Sydney NSW 2001