Privacy Statement

Zircon Financial Service (Australia) Pty Ltd • ACN 672 642 054 • AFSL 562700

This Privacy Statement is made on behalf of Zircon Financial Service (Australia) Pty Limited (ACN 672 642 054, Australian Financial Services Licence (**AFSL**) number 562 700) (**Zircon Australia**, **we**, **us** or **our**).

This Privacy Statement explains how Zircon Australia, and its related entities, collects, uses, maintains, protects and discloses your protect personal information, in accordance with the *Privacy Act 1988* (Cth) *(***Privacy Act***)*, the Australian Privacy Principles (**APPs**), *Privacy Regulation 2013 (Cth)* (**Privacy Regulation**) and the Office of the Australian Information Commissioner (**OAIC**) guidelines.

Zircon Australia is committed to protecting your privacy and maintaining compliance with the APPs contained within the Privacy Act. If there are any questions that arise in relation to this Privacy Statement do not hesitate to contact us.

Please read this Privacy Statement carefully before proceeding to provide Zircon Australia with your personal information. If you have any questions about this privacy statement, please contact us by emailing your question to contact@zr.au. We will review and make changes to this Privacy Statement from time to time to take into account new regulations and technology. It is important that you check our Privacy Statement regularly for any updates. If we make changes we consider to be important, we will let you know by placing a notice on our platform.

This Privacy Statement is available free of charge on Zircon Australia's website at zr.au and will be provided in any reasonable alternative form upon request.

Information we collect

The information we collect includes information, including personal information, you provide to us directly when visiting our website, platform, when completing the account opening application, in communications with us (including written and verbal correspondence) or ongoingly as we provide our services to you.

Zircon Australia generally collects personal information directly from you. However, in some circumstances, we may also collect personal information about you from third parties, including identity verification and credit reporting bodies, government agencies, your authorised agents or representatives, and our related entities. Where we collect personal information about you from a source other than you, we will take reasonable steps to notify you of the collection and its circumstances.

Personal information is information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from such information or opinion.

Zircon Australia will also collect personal information where required or authorised by or under Australian law, including the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**), the *Corporations Act 2001* (Cth) (**Corporations Act**), the *Income Tax Assessment Act 1997* (Cth), and any applicable court or tribunal order.

The information we collect may include:

- Name, date of birth, address, email address, contact number, tax file number, copy of any photo ID (including but not limited to driver's license, photo card, passport), bills/invoices/bank statements, bank account details, and any other information or documents that you provide to us.
- Information regarding your transactions with us, including your trading history using our services, your history of meeting margin calls, or your use of the various services and products provided by us.
- Information we obtain indirectly from you, including information gathered your interactions with our platform, website, application etc. This information includes but is not limited to Internet protocol (**IP**) address, browser type, operating system, Internet service provider, and time stamps.

Zircon Australia only collects personal information by lawful and fair means, which is reasonably necessary for the provision of our services when you provide it to us or when you use our website. In addition to the information listed above, Zircon Australia as part of its onboarding process and providing its services ongoingly requires that you provide demographic information from you when open an account, such as educational background and occupation, and relating to your trading experience, approximate annual income and approximate net worth to assess your financial position to assess whether you are within the scope of our target market.

You do not need to give us any of your personal information that is requested by Zircon Australia. However, if you do not provide the requested information, you will not be able to complete Zircon Australia's application form, and you will not be able to open an account, and we cannot provide you with any other services or information.

Sensitive information is a subset of personal information that is afforded a higher level of protection under the Privacy Act. Sensitive information includes information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information, biometric information, and biometric templates. Zircon Australia does not generally collect sensitive information in the ordinary course of providing its CFD services. Where Zircon Australia does collect sensitive information, it will only do so where:

(a) you have consented to the collection and the information is reasonably necessary for one or more of our functions or activities; or

(b) the collection is required or authorised by or under an Australian law or a court or tribunal order. Any sensitive information collected by Zircon Australia will be handled in accordance with the APPs and the heightened protections applicable to such information.

Where Zircon Australia receives personal information that it did not solicit, Zircon Australia will, where it is lawfully required and reasonable to do so, destroy or de-identify that information as soon as practicable.

External website links which may be found on the Zircon Australia website could lead to third party sites. If you access third party sites those sites may collect your information in a manner not specified in this Privacy Policy. Zircon Australia does not collect information about you from the third parties, you will need to contact them and ascertain what their privacy standards are.

How Zircon Australia uses and discloses your information

Zircon Australia uses your information to provide our services to you. We also use your information to provide you with updates on various matters regarding your use of our service, including margin obligations, your open trades, and other activities that may be applicable to you that are provided by Zircon Australia (**Primary Purpose**). Your information we collect, and use is to provide you with our services. We may also use or disclose your information for the following purposes:

(a) process your account application;

(b) perform our obligations to you;

(c) confirm your identity, create and administer your account, provide support functions, and contact you regarding your account to provide you with our services;

(d) execute and settle transactions you make on our platform;

(e) assess your suitability and appropriateness for our products and services;

(f) manage our market risk exposure and facilitate hedging arrangements with counterparties;

(g) detect and prevent fraud and other unlawful activities;

(h) report to AUSTRAC and other regulators as required by law;

(i) notify you of other products that may interest you;

(j) deliver statements to you;

(k) communicate with you regarding your activity using our services;

(l) carry out marketing and communications via email, text, the Zircon Australia application and other forms of communication. If you don’t want to receive marketing and offers from us, please unsubscribe from the communications via the link in our emails to you;

(m) analyse your information for the purpose of providing tailored services and marketing information, including to persons who we understand share similar interests and characteristics;

(n) improve our services and products;

(o) comply with government and regulatory requirements as required by law;

(p) organisations or individuals who you have informed us in writing are acting as your agent on your behalf;

(q) sharing your information with our:
   (i) agents, contractors or third-party service providers, to enable them to provide administrative and other support services to us; and/ or

   (ii) affiliates, if the information is required to provide the product or service you have requested, or to provide you with an opportunity to participate in their products or services;

(r) enabling us to meet our obligations under law, for example, the AML/CTF Act and Australian taxation laws; and

(s) related entities of Zircon Australia.

In the course of providing our services, Zircon Australia may disclose your personal information to different types of entities, included but not limited to the following:

(a) related entities of Zircon Australia, including its related entities in Hong Kong and Singapore;

(b) credit reporting and identity verification bodies;

(c) hedging counterparties;

(d) cloud service and technology providers;

(e) payment processors;

(f) external compliance auditors;

(g) government agencies and regulators (including AUSTRAC, ASIC and the ATO);

(h) external legal counsel;

(i) third-party service providers engaged by Zircon Australia for account processing, client surveys or data analysis; and

(j) your authorised agents or representatives.

Where we require your express consent, we will require your consent in writing, We may also disclose your personal information where it is required or authorised by law (such as to government agencies and regulatory bodies for law enforcement purposes).

If we disclose your personal information for a purpose other than providing you with our services (**Secondary Purpose**), then, subject to limited exceptions, that Secondary Purpose must be related to the Primary Purpose **and** one that you would **reasonably expect**. Where the personal information is sensitive information, the Secondary Purpose must be **directly** related to the Primary Purpose for which it was collected.

However, in certain instances Zircon Australia will use or disclose personal information for secondary purposes (in addition to the primary purpose). Personal information obtained to provide financial services may be applied to a secondary purpose if that respective purpose, is related to the primary purpose of collection and it is reasonable to expect the personal information to be used or disclosed for such secondary purpose.

For example: we may disclose your trading history to an external compliance auditor engaged to audit the quality of our services. This is permitted as it is directly related to the primary purpose of providing financial services and within your reasonable expectation as a client. However, we would not disclose your trading history to an unrelated third-party marketing company, as this would be outside your reasonable expectation and would not be related to the primary purpose.

Where Zircon Australia collects government-related identifiers (such as tax file numbers), we do so only where required or authorised by law, and handle such information in accordance with applicable legislation. Zircon Australia does not adopt any government-related identifier as its own identifier of an individual, and will only use or disclose a government-related identifier in the circumstances permitted by the APPs. An individual's name or Australian Business Number is not an a government-related identifier for the purposes of the Privacy Act and hence may be used to identify individuals.

Where a third party is engaged by us for the benefit of improving service provided to you, which may carry out account processing, fulfilment, client service, client satisfaction surveys or other data collection activities relevant to our business which may entail providing client information from our database. The provision of data is to analyse and identify client needs and notify clients of product and service offerings. Use of this information share is strictly limited to the performance of the tasks we directly request of the party and for no other un-approved process.

Zircon Australia requires all parties, if any, that have or has access to personal information to conform to our privacy standards.

You may direct us not to disclose your personal information to certain non-affiliated third parties. To opt out of sharing personal information with non-affiliated third parties, please contact a client service representative. An opt out election made by one account owner of a joint account is applicable to all account owners of the joint account. An opt out election must be made for each separate account you hold with us.

Use or disclosure of client personal information for **direct marketing purposes** is not permitted, unless either **express consent** has been obtained (e.g. at the time of client onboarding) or the person would reasonably expect their personal information to be used or disclosed for this purpose.

It is **not** sufficient to assume that the client would reasonably expect to receive the marketing material because of the client's profession, interest or hobby. The Australian Information Commissioner's view is that a person is not likely to have a reasonable expectation that their personal information will be used or disclosed for direct marketing purposes if the person has been notified that their personal information will only be used for a particular purpose unrelated to this.

If we wish to use our clients' personal information for the purpose of direct marketing, we include a consent to direct marketing in our standard fact finder, and always provide a means by which a client may request not to receive direct marketing communications (also known as 'opting out'), and comply with that request. This means that we must have a policy in place to track which clients do not want to receive direct marketing, and if a client has opted out of receiving direct marketing communications, we must ensure that they do not, in fact, receive direct marketing materials.

We may disclose a client's personal information for a purpose unrelated to providing financial advice if we have obtained our **client's written consent** to the disclosure.

When we disclose **personal information** of a client to a third party (e.g. external legal counsel), we ensure that the third party recipient signs a privacy agreement or acknowledgement whereby they agree to treat the personal information in accordance with the obligations set out in the privacy laws.

AML/CTF and KYC

Zircon Australia is a reporting entity under the AML/CTF Act and is required to verify the identity of all clients before providing its services to customers.

Zircon Australia is required by law – including the AML/CTF Act to verify the identity of all clients before providing services. Accordingly, you do not need to give us any of your personal information that is requested by Zircon Australia. However, if you do not provide the requested information, you will not be able to complete Zircon Australia's application form, and you will not be able to open an account, and we cannot provide you with any other services or information

Where Zircon Australia uses a credit reporting body to verify your identity, we will, before making the verification request, inform you of:

(a) the reasons for the request;

(b) the personal information that may be disclosed to the credit reporting body (being your name, residential address and date of birth);

(c) that we may request an assessment of whether that information matches information held by the credit reporting body;

(d) that the credit reporting body may prepare and provide such an assessment; and

(e) that the credit reporting body may use your information for the purpose of preparing that assessment.

We will obtain your express agreement before making any such request, and we will make an alternative means of identity verification available to you.

Records relating to identity verification are retained for a minimum of 7 years in accordance with our legal obligations.

Cookies

A cookie is a small text file placed on your computer hard drive by a web page server. Cookies may be accessed later by our web server. Cookies store information about your use of our web site. Cookies also allow us to provide you with more personalised service when using our web site.

Where required by applicable law, Zircon Australia will obtain your consent before placing non-essential cookies on your device. You may manage your cookie preferences through your browser settings or through our website cookie preference centre.

Zircon Australia may use cookies to:

- determine whether you have previously used the Zircon Australia website;
- identify the pages you have accessed; and
- facilitate administration of the site and for security purposes.

Most web browsers are set to accept cookies but you may configure your browser not to accept cookies. If you set your browser to reject cookies you may not be able to make full use of our website.

We may share web site usage information about visitors to the web site with reputable advertising companies for targeting our internet banner advertisements on the web site and other sites. For this purpose, pixel tags (also called clear gifs or web beacons) may be used to note the pages you have visited. The information collected by the advertising company through the use of these pixel tags is not personally identifiable.

To administer and improve our website, we may use a third party to track and analyse usage and statistical volume information, including page requests, form requests, and click paths. The third party may use cookies to track behaviour and may set cookies on behalf of us. These cookies do not contain any personally identifiable information.

E-mail address

If you provide us with your e-mail address during a visit to our website it will only be used for the purpose for which you provided it to us. It will not be added to a mailing list without your consent unless the mailing list is related to the purpose for which you provided your e-mail address to us. We may use your e-mail address, for example, to provide you with information about a particular service or respond to a message you have sent to us.

If you subscribe to one of our services and provide your e-mail address to us so that we may communicate with you through e-mail, we may also use your e-mail address to advise you of upgrades and changes to those services.

All commercial electronic messages sent by Zircon Australia comply with the *Spam Act 2003* (Cth), including requirements for consent, sender identification, and the provision of a functional unsubscribe facility in every commercial electronic message.

Accuracy of stored information

Zircon Australia takes reasonable steps to ensure the personal information held about certain individuals is accurate, up to date and complete. We verify personal information at the point of collection.

Zircon Australia also takes reasonable steps to ensure that personal information it uses or discloses is accurate, up-to-date, complete and relevant to the purpose for which it is used or disclosed.

Zircon Australia encourage you to help us wherever applicable by telling us immediately if you change your contact detail (such as your phone number, street address or email address) or if any of your details need to be corrected and or updated. A person wishing to update their personal information may contact our staff at contact@zr.au.

How we keep your information secure

Personal information is stored with security procedures in place. Personal information held electronically is protected by encryption, both in transit and at rest. Access to personal information is restricted on a need-to-know basis, with role-based access controls in place to ensure only authorised personnel can access relevant information

In the event hard copies of personal information are contained in hard copy files exist, these files are secured in an area whereby access is limited to authorised persons and employees of Zircon Australia.

External access of personal information by Zircon Australia's employees are under reasonable procedures to ensure the device being used on external networks has up to date, correct and current security updates installed. Zircon Australia also may consider, where necessary, the use of multi-factor authentication to ensure secure remote access.

Zircon Australia will shred or use secure paper disposal services for hard copy documents, in line with the information destruction process in place to ensure personal information is correctly destroyed.

We take reasonable steps and precautions to keep personal information secure from loss, misuse, and interference, and from unauthorised access, modification or disclosure.

If you use the internet to communicate with us, you should be aware that there are inherent risks in transmitting information over the internet. Zircon Australia does not have control over information while in transit over the internet and we cannot guarantee its security.

Zircon Australia retains personal information for as long as required to fulfil the purpose for which it was collected, and for the minimum periods required by law, being 7 years under the Corporations Act and the AML/CTF Act.

Where the information is no longer required to be held in or retained by Zircon Australia for any purpose or legal obligation, we will take reasonable steps to destroy or de-identify the information accordingly.

Access to personal information

Where a person requests access to their personal information, our policy, is to permit access, subject to certain conditions (as outlined below). Zircon Australia will correct personal information where that information is found to be inaccurate, incomplete or out of date. We shall not charge you a fee for your access request but may charge you the reasonable costs associated with processing your request.

If a person wishes to access their personal information or correct it, they should contact the Privacy Officer, and we will seek to provide such information and in the manner so requested (where reasonable to do so).

Zircon Australia may not always be able to give access to you, for all personal information we hold about you. If this is the case, we will provide you a written explanation of the reasons for our refusal, together with details of our complaints process for if you wish to challenge the decision.

We may not be able to give you access in instances where we believe the following:

- we reasonable believe this may pose a serious threat to the life, health of safety of any individual or to publish health/safety;
- it would unreasonably impact the privacy of another individual;
- such request is reasonably considered to be frivolous or vexatious;
- it relates to existing or anticipated legal proceedings which would otherwise not be accessible in the discovery process relating to such proceedings;
- it would reveal our intentions and thereby prejudice our negotiations with you;
- it would be unlawful;
- it is prohibited by some law or a court and or tribunal order;
- it relates to suspected unlawful activity or serious misconduct, access would likely prejudice the taking of appropriate action in relation to such activity and or misconduct;
- enforcement activities conducted by or on behalf of an enforcement body may be prejudiced; and/or
- access would reveal details regarding a commercially sensitive decision-making process.

We will respond to access requests within 30 days of receipt, unless the complexity of the request reasonably requires additional time, in which case we will notify you of the delay and the expected timeframe for response.

You may request access to information Zircon Australia holds about your identity verification by contacting our Privacy Officer at contact@zr.au.

Cross border disclosure and related anonymity

Zircon Australia may share, transfer or release personal information to its related entities overseas, including its related entities in Hong Kong and Singapore. Additionally, Zircon Australia may share your data to cloud service providers, technology vendors, AML/KYC and identity verification service providers, payment processors, and hedging counterparties who may be located in other jurisdictions.

Before disclosing your personal information to any overseas recipient, Zircon Australia takes reasonable steps to ensure that the overseas recipient handles your information in a manner consistent with the APPs, including through contractual arrangements with those recipients. Where Zircon Australia relies on such reasonable steps, Zircon Australia remains accountable under the Privacy Act for any acts or practices of the overseas recipient that would breach the APPs. Separately, Zircon Australia may disclose personal information to an overseas recipient without taking such reasonable steps where Zircon Australia reasonably believes that the recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the protection afforded by the APPs, and there are mechanisms that you can access to enforce that protection. Where Zircon Australia discloses your personal information in reliance on this exception, Zircon Australia is not accountable under the Privacy Act for any subsequent handling of your information by the overseas recipient.

Accuracy of personal information

Where Zircon Australia understands that:

- Personal information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading; and or

- You request us to correct personal information held about you.

Zircon Australia will take the reasonable steps to correct such information in a reasonable time frame. No fees are payable for such requests. If you request us to similarly advise a relevant third party for such correction, we will facilitate that notification unless impracticable or unlawful for us to do so.

If Zircon Australia intends to refuse to comply with your correction request, we will notify you in writing of our reasons for such refusal, and the complaints process you may avail if you wish to challenge that decision. You may also request that we associate the personal information we hold with a statement regarding your view of its inaccuracy.

Addressing a suspected or known data breach

A **data breach** occurs when **personal information** is accessed or disclosed in an unauthorised way or is lost.

A **data breach** could occur in a number of ways. Some examples include, but are not limited to:

- a mobile phone, laptop or removable storage device containing personal information is lost or stolen;
- sending an email containing personal information to the wrong recipient;
- accessing or disclosing personal information outside the requirements or authorisation of their employment;
- databases or an email account containing personal information are ‘hacked’ into or otherwise illegally accessed by an individual;
- a client file is lost or stolen; or
- paper records are stolen from insecure recycling or garbage bins.

Data breaches can give rise to a range of actual or potential harms to individuals and entities.

There are data breach reporting obligations that apply to any organisation covered by the privacy legislation.

Each breach is dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

The actions taken following a data breach generally follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach and evaluate the potential harm to affected individuals and, where possible, take action to remediate any risk of harm.

Step 3: Notify individuals and the OAIC if required. If the breach is an 'eligible data breach', such notification may be mandatory.

Step 4: Review the incident and consider what steps can be taken to prevent future breaches.

If remedial action is successful in preventing a likely risk of serious harm to individuals, the notification obligations may not apply.

An **eligible data breach** occurs when each of the following **three criteria** are satisfied:

a) there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;
b) this is likely to result in **serious harm** to one or more individuals; and
c) the entity has not been able to prevent the likely risk of serious harm with remedial action.

'**Serious harm'** is not defined in the legislation. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

We take into account the following (non-exhaustive) list of 'relevant matters' in assessing the likelihood of serious harm:

- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures, the likelihood that any of those security measures could be compromised
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security, technology or methodology:
  - was used in relation to the information; and
  - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information
- the likelihood that the persons, or the kinds of persons, who:
  - have obtained, or who could obtain, the information;
  - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates; and
  - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters.

Suspected Data Breach

Where Zircon Australia suspects (but has not confirmed) that an eligible data breach has occurred, we will conduct a reasonable and expeditious assessment and take all reasonable steps to complete that assessment within 30 days of becoming aware of the suspected breach.

If we confirm an eligible data breach has occurred, we will prepare a statement to the OAIC as soon as practicable. That statement will include:

(a) our identity and contact details;
(b) a description of the breach;
(c) the kinds of personal information involved; and
(d) the steps we recommend affected individuals take in response.

We will also notify affected individuals directly, or if that is not practicable, publish the statement on our website and via in-app notification.

Privacy complaints

If you have a complaint relating to our compliance with privacy laws or our treatment of your personal information, please contact us at complaints@zr.au. We will acknowledge your complaint within 24 hours of receipt and investigate it in accordance with our internal dispute resolution procedure. We will endeavour to resolve your complaint within 30 calendar days of receipt. If we require additional time, we will notify you of the reasons and provide an updated timeframe.

If you are not satisfied with the outcome of your complaint, you have the right to lodge a complaint with the Office of the Australian Information Commissioner by calling 1300 363 992 or visiting their website at **www.oaic.gov.au**.