Privacy Policy

About this Privacy Policy

This Privacy Policy is issued by Zircon Financial Service (Australia) Pty Ltd (ACN 672 642 054), the holder of Australian Financial Services Licence (**AFSL**) number 562700, trading as ZR Markets (**ZR Markets**, **we**, **us** or **our**).

It explains how we collect, use, hold, protect and disclose your personal information, in accordance with the *Privacy Act 1988* (Cth) (**Privacy Act**), the Australian Privacy Principles (**APPs**), the *Privacy Regulation 2013* (Cth) and the guidance of the Office of the Australian Information Commissioner (**OAIC**).

We are committed to protecting your privacy and to handling your personal information in accordance with the APPs. Please read this Privacy Policy before providing us with your personal information.

This Privacy Policy explains what information we collect, why we collect it, who we disclose it to, how we keep it secure, how long we keep it, and what you can ask us to do with it. It applies to our website at zr.au, our trading platform and applications, and to your dealings with us by telephone, email or other correspondence.

This Privacy Policy should be read alongside our Financial Services Guide, Product Disclosure Statement and User Agreement, all of which are available free of charge at zr.au. We will provide this Privacy Policy in any reasonable alternative form on request.

We review and update this Privacy Policy from time to time to reflect changes in law, technology and our business. The current version is always available at zr.au. Where we make a change we consider significant, we will notify you by placing a notice on our platform.

Can you deal with us anonymously?

You have the option of dealing with us anonymously or under a pseudonym for general enquiries — for example, if you contact us with a question about our products before opening an account.

However, we are required by the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act) to identify and verify every client before we provide a designated service. It is therefore not practicable for us to deal with you anonymously or under a pseudonym once you apply to open an account or once you become a client.

What information do we collect?

We collect personal information that you provide to us directly — when you visit our website or platform, complete an account application, correspond with us in writing or by phone, or in the course of us providing services to you.

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

The table below sets out the information we collect and why we collect it:

What we collect	Why we collect it
Identity and contact details	To establish and verify your identity, to open and administer your account, and to correspond with you about it. Includes your name, date of birth, residential and postal address, email address, telephone number, tax file number, and copies of identification documents such as a driver licence, photo card or passport.
Financial and verification records	To process deposits to and withdrawals from your account, and to establish the source of your funds. Includes your bank account details, proof of address documents such as utility bills or bank statements, and source of funds or source of wealth information.
Suitability and target market information	To assess whether our products are appropriate for you and whether you fall within our target market. Includes your educational background, occupation, trading experience and knowledge, approximate annual income and approximate net worth.
Account and trading records	To operate your account and to meet our record-keeping obligations. Includes your account activity, transaction and trading history, margin call history, and your use of the products and services we provide.
Technical information	To operate and secure our website, platform and applications. Includes your IP address, browser type, operating system, internet service provider and time stamps.

We generally collect personal information directly from you. In some circumstances we also collect personal information about you from third parties, including identity verification providers 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 the circumstances of it.

We collect personal information only by lawful and fair means, and only where it is reasonably necessary for our functions and activities. We also collect personal information where required or authorised by or under Australian law, including the AML/CTF Act, the Corporations Act 2001 (Cth) (Corporations Act), the Income Tax Assessment Act 1997 (Cth), and any applicable court or tribunal order.

You are not obliged to provide us with the personal information we request. However, if you do not provide it, you will not be able to complete our application form or open an account, and we will not be able to provide you with our services — in most cases because the law does not permit us to act without it.

Where we receive personal information that we did not solicit, and we could not have collected it under the APPs, we will destroy or de-identify that information as soon as practicable, provided it is lawful and reasonable to do so.

Do we collect sensitive information?

Sensitive information is a subset of personal information that attracts a higher level of protection under the Privacy Act. It includes information about an individual’s racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, criminal record, and health, genetic and biometric information.

We do not generally collect sensitive information in the ordinary course of providing our CFD services. Where we do collect sensitive information, we 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 by a court or tribunal order.

Any sensitive information we collect will be handled in accordance with the APPs and the heightened protections applicable to that information.

What about government-related identifiers?

Where we collect government-related identifiers such as tax file numbers, we do so only where required or authorised by law and handle them in accordance with the applicable legislation. We do not adopt a government-related identifier as our own identifier of an individual, and we will only use or disclose a government-related identifier in the circumstances permitted by the APPs. An individual's name and Australian Business Number are not government-related identifiers for the purposes of the Privacy Act.

How do we use your information?

We use your personal information to provide our services to you and to keep you informed about your account — including margin obligations, your open positions, and other activity relevant to the services we provide (**Primary Purpose**). In practice, we use your personal information to:

- process your account application and confirm your identity;
- create and administer your account and provide support functions;
- assess your suitability and appropriateness for our products and services, and monitor our target market determination;
- execute and settle the transactions you make on our platform;
- perform our obligations to you and deliver statements and confirmations;
- manage our market risk exposure and facilitate hedging arrangements with counterparties;
- detect, investigate and prevent fraud, market abuse and other unlawful activity;
- meet our obligations under law, including the AML/CTF Act, the Corporations Act and Australian taxation laws, and report to AUSTRAC, ASIC, the ATO and other regulators as required;
- communicate with you about your activity and about products and services that may be of interest to you, subject to section 7 below; and
- analyse and improve our products, services and platform.

Where we use or disclose your personal information for a purpose other than the Primary Purpose (a **Secondary Purpose**), that Secondary Purpose must — subject to limited exceptions — be related to the Primary Purpose and be one you would reasonably expect. Where the information is sensitive information, the Secondary Purpose must be directly related to the Primary Purpose.

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

Who do we disclose your information to?

In the course of providing our services, we disclose your personal information to the recipients set out below. We do not sell your personal information.

Recipient	Why we disclose
Related entities	Our related entities in Hong Kong and Singapore, for shared technology infrastructure and group support functions.
Identity verification and credit reporting bodies	To verify your identity as required under the AML/CTF Act, as described under "How do we verify your identity?" below.
Hedging counterparties and liquidity providers	To manage our market risk exposure arising from your transactions.
Technology and cloud service providers	To host, operate, secure and support our platform, website and records.
Payment processors	To process deposits to, and withdrawals from, your account.
Professional advisers	External legal counsel, auditors and external compliance auditors engaged by us.
Service providers	Third parties engaged by us for account processing, client service, client satisfaction surveys or data analysis.
Government agencies and regulators	Including AUSTRAC, ASIC, the ATO, law enforcement and courts or tribunals, where required or authorised by law.
Your representatives	Agents or representatives you have told us in writing are authorised to act on your behalf.

Where a third party is engaged by us, the use of your information is strictly limited to performing the tasks we request of that party, and for no other purpose. We require every party with access to personal information held by us to meet our privacy standards, and where we disclose personal information to a third party we ensure the recipient agrees in writing to handle that information in accordance with the privacy laws.

Where we require your express consent to a disclosure, we will obtain that consent in writing. We may also disclose your personal information where required or authorised by law, including to government agencies and regulatory bodies for law enforcement purposes.

You may direct us not to disclose your personal information to non-affiliated third parties. To opt out, contact our Client Service team. An opt-out election made by one account holder of a joint account applies to all holders of that account, and an opt-out election must be made separately for each account you hold with us.

How can you opt out of marketing?

We will only use or disclose your personal information for direct marketing purposes where you have given express consent — for example, at the time of onboarding — or where you would reasonably expect us to use your information for that purpose.

Every direct marketing communication we send identifies us as the sender and includes a simple means of opting out. If you no longer wish to receive marketing communications from us, you may unsubscribe using the link in our emails or by contacting our Client Service team. We maintain a record of each opt-out election so that it continues to be given effect. You may also ask us to tell you the source of the information we used, and we will do so free of charge within a reasonable period.

We will not disclose your personal information for a purpose unrelated to the financial services we provide unless we have obtained your written consent to that disclosure.

How do we verify your identity?

We are a reporting entity under the AML/CTF Act and are required to identify and verify every client before providing a designated service.

Where we use 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. You may request access to the information we hold about your identity verification by contacting our Client Service team at clientservice@zr.au.

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

How do we use cookies and analytics?

A cookie is a small text file placed on your device by a web server and later read by that server. Cookies store information about your use of our website and allow us to provide a more personalised service. We use cookies to:

- recognise whether you have previously used our website;
- identify the pages you have accessed; and
- administer the site and support its security.

Where required by applicable law, we will obtain your consent before placing non-essential cookies on your device. You can manage your preferences through your browser settings or through the cookie preference centre on our website. Most browsers are set to accept cookies by default; if you configure your browser to reject them, you may not be able to make full use of our website.

We may engage third parties to track and analyse website usage and statistical information, including page requests, form requests and click paths. These third parties may set cookies on our behalf. The information collected through this analytics activity is not personally identifiable.

Where we use marketing or advertising cookies and similar technologies, including pixel tags (also known as clear GIFs or web beacons), we will do so only with your consent through our cookie preference centre. These technologies may be set by third-party advertising providers to measure the effectiveness of our advertising and to show you our advertisements on other websites.

Our website may contain links to third-party websites. Those sites may collect your information in ways not described in this Privacy Policy, and we are not responsible for their privacy practices. We recommend you review the privacy policy of any third-party site you visit.

How do we handle email and electronic messages?

If you provide your email address when visiting our website, we will use it only for the purpose for which you provided it. It will not be added to a mailing list without your consent, unless that mailing list is related to the purpose for which you gave us the address. If you subscribe to one of our services, we may also use your email address to notify you of upgrades and changes to those services.

All commercial electronic messages we send comply with the *Spam Act 2003* (Cth), including its requirements for consent, sender identification and a functional unsubscribe facility in every message.

Do we disclose your information overseas?

We may transfer or disclose personal information to recipients located outside Australia, including:

- our related entities in Hong Kong and Singapore;
- cloud service providers and technology vendors;
- AML/KYC and identity verification service providers;
- payment processors; and
- hedging counterparties and liquidity providers.

Before disclosing your personal information to an overseas recipient, we take reasonable steps to ensure that the recipient handles your information in a manner consistent with the APPs, including through contractual arrangements with that recipient. Where we rely on those reasonable steps, we remain accountable under the Privacy Act for any act or practice of the overseas recipient that would breach the APPs.

Separately, we may disclose personal information to an overseas recipient without taking those steps where we reasonably believe the recipient is subject to a law, or a binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the APPs, and where there are mechanisms you can access to enforce that protection. Where we disclose your personal information in reliance on that exception, we are not accountable under the Privacy Act for the subsequent handling of your information by that recipient.

How do we keep your information secure, and how long do we keep it?

Personal information held electronically is protected by encryption, both in transit and at rest. Access is restricted on a need-to-know basis, with role-based access controls so that only authorised personnel can access relevant information. Where our personnel access personal information from outside our network, we require the device used to have current security updates installed, and we use multi-factor authentication for remote access.

Where hard copy files containing personal information exist, they are stored in an area to which access is limited to authorised personnel. Hard copy documents are shredded or destroyed using secure paper disposal services in line with our information destruction process.

We take reasonable steps to protect personal information from misuse, interference and loss, 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. We do not control information while it is in transit and cannot guarantee its security.

We retain personal information for as long as it is required for the purpose for which it was collected, and for the minimum periods required by law — being seven years under the Corporations Act and the AML/CTF Act. Where information is no longer required for any purpose or legal obligation, we take reasonable steps to destroy or de-identify it.

How can you access and correct your information?

You may exercise the following rights at any time:

You may ask us to	How to do so, and what happens next
Provide access to what we hold	Contact our Client Service team at clientservice@zr.au. We do not charge a fee for making an access request, although we may charge you the reasonable costs of processing it. We will respond 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 our response.
Correct your information	Contact our Client Service team at any time, and in particular if your contact details change. We will correct the information within a reasonable time and at no cost to you, and will notify any third party to whom we have disclosed it if you ask us to.
Stop marketing to you	Use the unsubscribe facility in any marketing communication from us, or contact our Client Service team.
Provide an alternative means of identity verification	Contact our Client Service team if you do not wish us to verify your identity through a credit reporting body.
Deal with us anonymously	You may make general enquiries without identifying yourself. This is not available once you apply to open an account.

We take reasonable steps to ensure the personal information we hold, use and disclose is accurate, up to date, complete and relevant to the purpose for which it is used or disclosed, and we verify personal information at the point of collection. Your cooperation helps us keep our records accurate, so please tell us promptly if your details change.

Where we are satisfied that information we hold is inaccurate, out of date, incomplete, irrelevant or misleading, or where you ask us to correct it, we will take reasonable steps to correct it within a reasonable time and at no cost to you. If you ask us to notify a third party of the correction, we will do so unless it is impracticable or unlawful.

When can we refuse a request?

We may not always be able to give you access to all of the personal information we hold about you. Where we refuse, we will give you a written explanation of our reasons together with details of our complaints process, so that you can challenge the decision if you wish. The same applies if we refuse a correction request; you may also ask us to associate a statement with the information setting out your view that it is inaccurate.

We may refuse access where, for example:

- giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of another individual;
- the request is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings and would not be accessible through the discovery process in those proceedings;
- giving access would reveal our intentions in relation to negotiations with you and prejudice those negotiations;
- giving access would be unlawful, or is prohibited by law or by a court or tribunal order;

- the information relates to suspected unlawful activity or serious misconduct and access would be likely to prejudice appropriate action being taken;
- giving access would be likely to prejudice enforcement activities conducted by or on behalf of an enforcement body; or
- giving access would reveal evaluative information generated in connection with a commercially sensitive decision-making process.

What happens if there is a data breach?

A **data breach** occurs where personal information we hold is lost, or is accessed or disclosed without authorisation. We maintain a Data Breach Response Plan and assess each incident on its own facts, following four steps: we contain the breach; we assess it and the potential harm to affected individuals; we notify where notification is required; and we review the incident to prevent a recurrence.

Where we suspect but have not confirmed that an **eligible data breach** has occurred, we will carry out a reasonable and expeditious assessment and take all reasonable steps to complete it within 30 days of becoming aware of the suspected breach. An eligible data breach occurs where there is unauthorised access to or disclosure of personal information, or a loss of personal information, that is likely to result in serious harm to one or more individuals, and we have not been able to prevent that likely risk of serious harm through remedial action.

If we confirm an eligible data breach has occurred, we will prepare a statement for the OAIC as soon as practicable, setting out our identity and contact details, a description of the breach, the kinds of personal information involved, and the steps we recommend affected individuals take in response. We will also notify affected individuals directly or, where that is not practicable, publish the statement on our website and issue an in-app notification.

How do you make a privacy complaint?

If you are not satisfied with how we have handled your personal information, or with our compliance with the privacy laws, you may make a complaint to us at complaints@zr.au.

We will acknowledge your complaint within one business day of receipt and investigate it under our internal dispute resolution procedure. We will endeavour to provide you with a response within 30 calendar days of receipt. If we need more time, we will notify you of the reasons and give you an updated timeframe.

If you are not satisfied with the outcome of your complaint, you may lodge a complaint with the Office of the Australian Information Commissioner on 1300 363 992 or at www.oaic.gov.au.