Privacy Policy

capital•com

Privacy Policy

1. About us

Capital Com Australia Pty Ltd ('we', 'our', 'us', the 'Company') is a company registered in Australia and is licensed as an Australian Financial Services Licensee under AFSL 513393. We are bound by the Privacy Act 1988 (Privacy Act), including the Australian Privacy Principles (APPs) and recognise the importance of ensuring the confidentiality and security of your personal information. Our contact details are as follows:

Licensee name: Capital Com Australia Pty Ltd

AFSL number: 513393

Address: Level 15, 357 Collins Street, Melbourne, 3000, Victoria

Website: www.capital.com

Email: compliance.au@capital.com

2. Introduction

In this Privacy Policy:

- Associated Companies means companies within the Capital.Com group or partners (located in the countries listed under Sending personal information overseas, as updated from time to time) and any future companies added to this group;
- Disclosure of information means providing information to third parties or persons outside of our Company;
- Personal information means information or an opinion relating to an individual, which can be used to identify that individual;
- Privacy Officer means the contact person within our Company for questions or complaints regarding how we handle personal information;
- Sensitive information is personal information that includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences and criminal record, and also includes health information; and
- Use of information means use of information within our Company or our associated companies.

3. Your rights

This Privacy Policy contains information about how:

- you may access the personal information we hold about you;
- you may seek the correction of your personal information;
- you may ask us to provide an alternative means of identity verification for the purposes of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth);
- you may complain about a breach of the Privacy Act, including the APPs; and
- we will deal with a privacy complaint.

4. What personal information do we collect and hold?

We may collect and hold a range of personal information about you to provide you with our services, including your:

- name;
- address;
- phone numbers;
- email addresses;
- occupation;
- bank account details;
- driver's licence or other identity document details;
- financial information, including details of:
  - your investments; and
  - taxation information.

5. How we collect personal information

We generally collect personal information directly from you. For example, personal information will be collected through our application processes, forms and other interactions with you in the course of providing you with our products and services, including when you visit our website or social media pages, use a mobile app from us, call us or send us correspondence via email or live chat.

We may also collect personal information about you from a third party, such as electronic verification services, partners, affiliates and introducing brokers ('Referrers') or marketing agencies. If so, we will take reasonable steps to ensure that you are made aware of this Privacy Policy. We may also use third parties to analyse traffic at our website, which may involve the use of cookies. Information collected through such analysis is anonymous.

We will not collect sensitive information about you without your consent unless an exemption in the APPs applies. These exceptions include if the collection is required or authorised by law, or necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct.

If the personal information we request is not provided by you, we may not be able to provide you with the benefit of our services or meet your needs appropriately.

We do not give you the option of dealing with us anonymously, or under a pseudonym. This is because it is impractical, and, in some circumstances, illegal for us to deal with individuals who are not identified.

6. Unsolicited personal information

We may receive unsolicited personal information about you. We will destroy or de-identify all unsolicited personal information we receive unless it is relevant to our purposes for collecting personal information. We may retain additional information we receive about you if it is combined with other information we are required or entitled to collect. If we do this, we will retain the information in the same way we hold your other personal information.

7. Who we collect personal information about

The personal information we may collect and hold includes (but is not necessarily limited to) personal information about:

- our clients;
- potential clients;
- service providers or suppliers;
- prospective employees, employees and contractors; and
- other third parties with whom we come into contact such as Referrers.

8. Website Collection

We collect personal information from our website www.capital.com when we receive emails and online forms. For more information, please refer to our Cookie Policy.

We use cookies to understand how users interact with our website, to compile aggregate data about our website traffic, including where our website visitors are located, and interaction so that we can offer better user experiences. In addition we use Marketing cookies to enable you to experience more relevant online content and see adverts which are aligned with your interests.

Cookies are mainly stored on your side; this means that you are generally able to delete them at any time. You can use your website browser settings to accept, refuse and delete cookies. To do this, follow the instructions provided by your browser or for general information on how to remove cookies, please visit: www.aboutcookies.org which has instructions on how to amend your cookie settings for a variety of browsers and how to delete existing cookies from your computer.

Cookies do not contain personal information in themselves but can be used to identify a person when combined with other information. Cookies are small text files which are transferred to your computer's hard drive through your web browser that enables our website to recognise your browser and capture and remember certain information. This includes facilitating your use of our website and mobile application by completing forms or other inquiries and from maintaining records of information provided in the course of ongoing customer support. We may acquire information from other sources i.e. credit information, identity checks, questionnaires, user interactions.

We provide our clients with 2 types of cookie identifiers, "session cookies" which are short term and "third party cookies" which are long term. The cookies which we store are only related to device identifiers (i.e. IPs, OS, browser) and they are not related to any of your personal information client personal data.

In addition to our use of cookies, we may record any communications, electronic, by telephone, LiveChat or otherwise, that we have with you in relation to the services we provide to you.

Whilst we do not currently use third parties to analyse traffic at that website, we reserve the right to do so in future and will update our Privacy Policy accordingly. Information collected through such analysis is anonymous.

9. Why we collect your personal information

We may use and disclose the information we collect about you for the following purposes:

- to provide you with our products and services;
- to review and meet your ongoing needs;
- to provide you with information we believe may be relevant or of interest to you;
- to let you know about other products or services we offer, send you information about special offers or invite you to events;
- to consider any concerns or complaints you may have;
- to comply with relevant laws, regulations and other legal obligations; and
- to help us improve the products and services offered to our customers and enhance our overall business.

We may use and disclose your personal information for any of these purposes. We may also use and disclose your personal information for secondary purposes which are related to the primary purposes set out above, or in other circumstances authorised by the Privacy Act.

Where applicable, sensitive information will be used and disclosed only for the purpose for which it was provided (or a directly related secondary purpose), unless you agree otherwise, or an exemption in the Privacy Act applies.

10. Who we might disclose your personal information to

We may disclose personal information to:

- our Associated Companies;
- an agent, contractor or service provider we engage to carry out functions and activities for or on our behalf, such as our lawyers, accountants, debt collectors or other advisers;
- organisations involved in managing payments, including payment merchants and other financial institutions, such as banks;
- regulatory bodies, government agencies, law enforcement bodies, the Australian Financial Complaints Authority (AFCA) and courts;
- financial product issuers and credit providers;
- anyone else to whom you authorise us to disclose it or is required by law; and
- our Referrers (if applicable).

If we disclose your personal information to service providers or our Associated Companies that perform business activities for us, they may only use your personal information for the specific purpose for which we supply it. We will ensure that all contractual arrangements with third parties adequately address privacy issues, and we will make third parties aware of this Privacy Policy.

We may disclose the following personal information to credit reporting bodies ('CRB'), to comply with our obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF obligations):

- name;

- date of birth; and
- residential address.

The purpose of disclosing this information is to enable us to verify whether the personal information collected matches the identification information held by the CRB. We may, upon request, provide you with an alternative method of verification, however, any alternative verification method must also comply with the AML/CTF legislation.

To verify your identity, we may disclose details from your identity documents (such as your passport, driver's licence or other government-issued identity document) to the document issuer or official record holder through the Document Verification Service (DVS). The check is made on our behalf by third-party identity verification service providers, including gateway service providers that connect to the DVS and providers that help us collect and check identity documents. The DVS confirms whether the details you provide match the records held by the document issuer; it does not provide us with any further information held by the issuer. The result of the check is recorded on your client file, which may be accessed by authorised personnel of our Associated Companies as described under Sending personal information overseas below. You can find more information about the operation of the DVS at www.idmatch.gov.au.

11. Sending personal information overseas

We may disclose personal information within our group and other associated companies that may be located outside Australia in some circumstances. We require our associates to acknowledge the confidentiality of the clients personal information and to respect any individual's right of privacy and comply with either the Australian Privacy Principles or their local privacy regime and this privacy notice.

The personal information we disclose to our Associated Companies may include identity verification information, including the outcome of checks made through the Document Verification Service. This information may be accessed by authorised personnel of our Associated Companies, on a need-to-know basis and only where required to perform compliance, onboarding and anti-money laundering functions on our behalf. These Associated Companies are located in the United Kingdom, Cyprus, Bulgaria, Poland, Lithuania, Italy, Gibraltar, Switzerland, the United Arab Emirates, the Bahamas, Bermuda, Canada, Chile, Brazil, South Africa, Kenya, Singapore and Japan. We will update this Privacy Policy before personnel located in any other country are given access to this information.

We will not send personal information to recipients outside of Australia unless:

- we have taken reasonable steps to ensure that the recipient does not breach the Act and the APPs;
- the recipient is subject to an information privacy scheme similar to the Privacy Act; or
- the individual has consented to the disclosure.

If you consent to your personal information being disclosed to an overseas recipient, and the recipient breaches the APPs, we will not be accountable for that breach under the Privacy Act, and you will not be able to seek redress under the Privacy Act.

12. Managing personal information

We recognise the importance of securing the personal information of our clients and will take the necessary steps to ensure your personal information is protected from misuse, interference or loss, and unauthorised access, modification or disclosure.

Your personal information is generally stored in our computer database. Any paper files are stored in secure areas. In relation to information that is held on our computer database, we apply the following guidelines:

- passwords are required to access the system and passwords are routinely checked;
- data ownership is clearly defined;
- we change employees' access capabilities when they are assigned to a new position;
- employees have restricted access to certain sections of the system;
- the system automatically logs and reviews all unauthorised access attempts;
- unauthorised employees are barred from updating and editing personal information;
- all computers which contain personal information are secured both physically and electronically;
- data is encrypted during transmission over the network; and
- print reporting of data containing personal information is limited.

Where our employees work remotely or from home, we implement the following additional security measures:

- two-factor authentication is enabled for all remote working arrangements;
- password complexity is enforced, and employees are required to change their password at regular intervals;
- we ensure that employees only have access to personal information which is directly relevant to their duties;
- employees are not permitted to work in public spaces or to access our systems through public WIFI;
- we use audit trails and audit logs to track access to an individual's personal information by an employee;
- we monitor access to personal information, and will investigate and take appropriate action if any instances of unauthorised access by employees are detected;
- employees must ensure that screens are angled so that they cannot be used by anyone else, and are locked when not in use;
- employees must ensure that no other member of their household uses their work device;
- employees must store devices in a safe location when not in use;
- employees may not make hard copies of documents containing personal information, nor may they email documents containing personal information to their personal email accounts; and
- employees may not disclose an individual's personal information to colleagues or third parties, via personal chat groups.

13. Direct marketing

We may only use personal information we collect from you for the purposes of direct marketing without your consent if:

- the personal information does not include sensitive information; and
- you would reasonably expect us to use or disclose the information for the purpose of direct marketing; and
- we provide a simple way of opting out of direct marketing; and
- you have not requested to opt out of receiving direct marketing from us.

If we collect personal information about you from a third party, we will only use that information for the purposes of direct marketing if you have consented (or it is impracticable to obtain your consent), and we will provide a simple means by which you can easily request not to receive direct marketing communications from us. We will draw your attention to the fact you may make such a request in our direct marketing communications.

You have the right to request us not to use or disclose your personal information for the purposes of direct marketing, or for the purposes of facilitating direct marketing by other organisations. We must give effect to the request within a reasonable period. You may also request that we provide you with the source of their information. If such a request is made, we must notify you of the source of the information free of charge within a reasonable period.

14. Contractual arrangements with third parties

We ensure that all contractual arrangements with third parties adequately address privacy issues, and we make third parties aware of this Privacy Policy.

Third parties will be required to implement policies in relation to the management of your personal information in accordance with the Privacy Act. These policies include:

- regulating the collection, use and disclosure of personal and sensitive information;
- de-identifying personal and sensitive information wherever possible;
- ensuring that personal and sensitive information is kept securely, with access to it only by authorised employees or agents of the third parties; and
- ensuring that the personal and sensitive information is only disclosed to organisations which are approved by us.

15. How we keep personal information accurate and up-to-date

We are committed to ensuring that the personal information we collect, use and disclose is relevant, accurate, complete and up-to-date.

We encourage you to contact us to update any personal information we hold about you. If we correct information that has previously been disclosed to another entity, we will notify the other entity within a reasonable period of the correction. This Privacy Policy will be reviewed from time to time to take account of new laws and technology, and changes to our operations and the business environment. Where we have made material changes to this policy, we will notify you of those changes.

16. Accessing your personal information

Subject to the exceptions set out in the Privacy Act, you may gain access to the personal information that we hold about you by contacting our Privacy Officer. We will provide access within 30 days of your request. If we refuse to provide the information, we will provide reasons for the refusal.

We will require identity verification and specification of what information is required. An administrative fee for search and photocopying costs may be charged for providing access at our sole discretion.

17. Updates to our Privacy Policy

This Privacy Policy will be reviewed from time to time to take account of new laws and technology, and changes to our operations and the business environment. Where we have made material changes to this policy, we will notify you of those changes.

18. Responsibilities

It is the responsibility of management to inform employees and other relevant third parties about this Privacy Policy. Management must ensure that employees and other relevant third parties are advised of any changes to this Privacy Policy. All new employees are to be provided with timely and appropriate access to this Privacy Policy, and all employees are provided with training in relation to appropriate handling of personal information. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

19. Non-compliance and disciplinary actions

Privacy breaches must be reported to management by employees and relevant third parties. Ignorance of this Privacy Policy will not be an acceptable excuse for non-compliance. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

20. Complaints

We have an effective complaint handling process in place to manage privacy risks and issues. For more information about our complaints handling process, please refer to our Complaints Policy which is available on our website.

The complaints handling process involves:

- identifying (and addressing) any systemic/ongoing compliance problems;
- increasing consumer confidence in our privacy procedures; and
- helping to build and preserve our reputation and business.

You can make a complaint to us about the treatment or handling of your personal information by lodging a complaint with the Privacy Officer.

If you have any questions about this Privacy Policy, or wish to make a complaint about how we have handled your personal information, you can lodge a complaint with us by:

Email: complaints.au@capital.com
Live chat: https://capital.com/contact-us

If you are not satisfied with our response to your complaint, you can also refer your complaint to the Office of the Australian Information Commissioner ('OAIC') by:

Telephone: 1300 363 992

Post: Director of Complaints, Office of the Australian Information Commissioner, GPO Box 5218, SYDNEY NSW 2001

E-mail: enquiries@oaic.gov.au