

Privacy Policy - Australia

Table of Contents

1.	Introduction	3
2.	Scope	3
3.	Personal Information	3
3.1	Sensitive Information	4
4.	Collection of Personal Information	4
5.	Storage of Personal Information	4
6.	Accessing your Information	5
7.	Retention of Personal Information	5
8.	Disclosure, Sharing and Transfer of Personal Information Overseas	5
9.	Security of Personal Information	6
10.	Consent to Personal Data Collection, Use, and Disclosure	6
11.	Updates to the Data Protection Policy	7
12.	Third Party Websites	8
13.	Complaints	8
14.	ANNEXURE A – Notifiable Data Breaches ('NDB') Policy	9
14.1	What is an Eligible Data Breach (EDB)?	9
14.2	What is a Data Breach?	9
14.3	Serious Harm	10
14.4	Types of Personal Data and Serious Harm	10
14.5	Reporting a Data Breach	10
14.6	The OAIC Form for lodging Statements to the Commissioner	10
14.7	Notifying AUSTRAC or the Australian Cyber Security Centre of an EDB	10

Privacy Policy - Australia

1. Introduction

CITIC Securities Australia Pty Ltd (formerly known as CLSA Australia Pty Ltd) (”CSA”) recognises the importance of the personal information (as defined in Australian Privacy Act 1988) we hold about you or any natural persons’ personal information provided by you and the trust they place in us.

By explaining our Privacy Policy (“Policy”) to you, we hope that you will better understand how we keep personal information private and secure while using it to provide services and products.

We are committed to safeguarding your personal information in accordance with the requirements of the Australian Privacy Act 1988, Privacy Regulation 2013, Australian Privacy Principles contained in the Australian Privacy Act 1988 and the Australian Notifiable Data Breaches scheme and any other applicable personal information protection rules or laws, which all regulate the way individual’s personal information is handled (“personal information protection laws”).

In general, we will not use or disclose such information collected about you otherwise than for the purposes set out in this Policy, for a purpose you would reasonably expect, a purpose required or permitted by law, or a purpose otherwise disclosed to, or authorised by you.

2. Scope

This Policy applies to the Australian operations of the group of CITIC Securities International (“CSI”) including (i) CSI and all the entities, at any time directly or indirectly, controlling, controlled by or under common control with CSA or (ii) controlled by CSI (collectively “CSI Group”) unless specifically stated otherwise and captures all employees, contractors and other authorised third parties who have access to any personal information held by or on behalf of the CSA.

3. Personal Information

CSA collects relevant data that is essential to provide financial services or products to its clients.

Most of the personal information collected and outlined in this Policy are regulatory requirements, for example, CSA must evidence we have confirmed the identify of our clients in accordance with the Australian Anti-Money Laundering and Counter Terrorism Financing (“AML/CFT”) Act and rules.

To ensure financial services are effectively provided, the following types of standard Personal Information may be collected from you:

- name;
- address;
- date of birth;
- gender;
- nationality;
- residency status;
- telephone number;
- e-mail address;
- financial information;
- tax file number;
- employment history;
- education history;
- information contained in identity document, such as a passport number and drivers licence number;

- information necessary to make or receive payments to or from you or necessary to effect security transactions on your behalf; and/or
- any other information as required to comply with the applicable regulations or laws or required to provide the services.

3.1 Sensitive Information

The following Personal Information is regarded as sensitive:

- racial or ethnic origin;
- political opinion or membership of political association;
- religious or philosophical beliefs;
- health;
- membership of professional or trade associations or trade union; and
- criminal record.

4. Collection of Personal Information

Authorised employees of CSA or any of our related entities within the CSI group are authorised to collect personal information. No department or individual within CSA or CSI group may process personal information for any reason other than for the lawful purposes for which it was collected and is being processed.

Generally, the CSI Group collects, uses and discloses Personal Information for the following purposes:

- Processing applications for account opening purposes
- Account maintenance and operational duties relating to your account(s)
- Processing of transactions
- Managing your relationship with CSI group
- Carrying out our client's instructions or responding to our clients
- Preventing, detecting and investigating any misconduct or unlawful activities
- Complying with all applicable laws, regulations, rules etc.
- Addressing or investigating a complaint, claims or disputes;
- Provision of financial services;
- Managing our infrastructure and business operations and employees and complying with our policies and procedures that may be required by applicable laws and regulations including those relating to risk control, compliance, security, audit, finance and accounting, human resources, systems and business continuity;
- Carrying out research, planning and statistical analysis;
- organising promotional events;
- Enforcing our legal and/or contractual rights against you including, but not limited to, recovering any and all amounts owed to us or any members of the CSI group.

5. Storage of Personal Information

Your personal information may be held within our (or our service providers):

- premises in paper records;
- computer systems including email, servers, hard drives and applications;
- data storage systems; and
- in certain circumstances, in sound recordings of your telephone discussions with CSA.

6. Accessing your Information

If at any time you would like to request access and/or make corrections, or withdraw consent, you are welcome to ask us in a form or manner which identifies the nature of the personal information requested.

Requests can be made to your CSA business contact or the Privacy Officer for the Australian operation of CSA as follows:

Email: compliance_australia@clsa.com

Mail: The Privacy Officer
CITIC Securities Australia Pty Ltd
Level 35, Grosvenor Place
Sydney NSW 2000

Tel: +61 2 8571 4200

Generally, we will provide you with access to the personal information we hold about you within a reasonable time. Under certain circumstances however, we may not be able to provide you with access to the personal information we hold about you. This includes where:

- it would have an unreasonable impact on the privacy of another individual;
- the request is frivolous or vexatious;
- information relates to legal proceedings;
- the information would reveal a commercially sensitive decision-making process; or
- we are prevented by law from disclosing the information, or providing access would prejudice certain investigations.

Unless we are unable to do so, we will inform you of the reason(s) for refusing access.

We may charge a fee for providing access to your personal information

7. Retention of Personal Information

Personal information will be held for as long as it is necessary to fulfil the purpose for which is was collected or as required by applicable laws. The maximum retention period for personal information is seven years.

8. Disclosure, Sharing and Transfer of Personal Information Overseas

As a global financial institution, our services are supported by certain entities within the CSI group. These entities process your data as necessary to operate effectively, efficiently, and securely in facilitating transactions and providing products and services to our clients.

From time to time, we may also send your personal data overseas whenever it is necessary for the performance of, but not limited to, providing products and services to you, fulfilling the client agreement,

complying with legal requirements, or conducting direct marketing activities. Such transfers may involve sharing your data offshore working for us that operate or store data outside your local jurisdiction. Where your information is sent overseas, it is likely to be in the following jurisdictions: Hong Kong, China, Singapore, Thailand, Philippines, Indonesia, Malaysia, Japan, Korea, India, the Netherlands, the United Kingdom, and the United States.

Subject to the provisions of applicable laws in each region the CSI group operates in, your personal information may be disclosed or transferred to or shared with or retained by the following:

- Related entity of the CSI group;
- Any third party service provider;
- Our professional advisors (including our lawyers) and agents or third parties necessary for us performing/providing services to you (including our executing brokers, clearing houses and settlement agents);
- Our auditors;
- Any person to whom disclosure is permitted or required by law or any court order;
- Any local or foreign government agency, regulatory authority who have jurisdiction over CSI; and/or
- Any successors and assigns, whether located in or outside the relevant jurisdiction

The personal data that we collect from you may be transferred to, and stored at, a destination outside Australia. It may also be processed by individuals operating outside your local jurisdiction who work for CSI group. This includes jurisdiction that may not have the same level of protection for personal data. At CSA, we are committed to protecting your personal data and your privacy. Where your personal data is sent outside your local jurisdiction, it will be handled in accordance with that jurisdiction's applicable data protection laws. We will ensure that appropriate data handling, security measures, and legal safeguards are in place. We employ a range of measures to keep your information safe and secure, which may include encryption and other security measures. Our employees and any third parties who carry out work for us must comply with appropriate compliance standards, including the responsibility to protect any information and implement appropriate measures for its use and transfer.

9. Security of Personal Information

CSA will take reasonable steps to protect the Personal Information it holds from interference, misuse and loss and from unauthorised access, modification or disclosure. In line with our internal authorisation and access policies, employees only have access to information on a need to know basis.

To the extent permitted by law, CSA will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used and disclosed under this Policy except in circumstances where CSA is required or authorised to retain such Personal Information (including as a result of the operation of tax, financial services or other applicable laws).

10. Consent to Personal Data Collection, Use, and Disclosure

Your consent governs our use of your personal information, including for the following purposes:

10.1 Direct Marketing

We may, from time to time, and with your consent as required by personal information protection laws, use the personal data provided by you for direct marketing purposes. In this regard, please note that:

(i) Your personal data, including your name, contact details (such as email addresses and phone numbers), product and service preferences, transaction history, financial background, and demographic data, may be used by CSA and shared with the CSI group, or with third-party subcontractors, agents, or service providers work for us, whether located locally or overseas, for the purposes of direct marketing.

(ii) The types of services, products, and subjects that may be marketed to you, whether currently available or developed in the future by CSA or the CSI group, include:
- News, updates, offers, and promotional information;
- Investment, financial, insurance products or services; and
- Privilege programs, along with related offerings; and
- Products and services provided by our co-branding partners.

(iii) The above services, products, and subjects may be communicated or solicited through the following channels:
- Email, telephone, mobile application, SMS and other electronic means
- Either directly to you or through your representatives/contact persons, if you are a corporate entity.

10.2 Data Disclosure

By interacting with CSA and submitting information to us or signing up for any financial services for financial products offered by us you agree and consent to:

- CSA collecting, using, disclosing and sharing your personal information as stated under this Policy;
- Disclosing and sharing such personal information to the CSA/CSI Group's authorised service providers and relevant third parties.

If you do not wish for us to continue to use your Personal Data or the Personal Data provided by you to us for any of the Purposes at any time in the future, you must notify us in writing addressed to the Data Protection Officer to withdraw your consent. Depending on the circumstances, your withdrawal of consent may result in CSA's inability to provide you with the services and/or products that we have been offering to you, and consequently, may result in the termination of your relationship and/or accounts with us.

Under relevant circumstances where the personal information protection laws permit us to collect, use, process, transfer or disclose the personal information of you without your consent, such permission or rights granted by the law shall continue to apply notwithstanding anything herein to the contrary.

11. Updates to the Data Protection Policy

CSA may from time to time update this Policy to ensure that it is consistent with our future developments, industry trends and/or any changes in legal or regulatory requirements. Such changes will be posted on our web-site.

Your continued use of our service will be taken as acceptance of the updated Policy.

12. Third Party Websites

Our corporate web site may contain links to other web-sites. Please note that we are not responsible for the privacy practices of such other web sites and you are advised to read the privacy statement of each web site you visit which may collect your Personal Information.

13. Complaints

If you wish to make a complaint about our collection, use or disclosure of your personal information, you should contact your CSA contact or our Privacy Officer in writing (see section 6 above).

We will make every effort to resolve your complaint internally within a reasonable time.

If we do not resolve your complaint to your satisfaction, you may contact the Office of the Information Commissioner (OAIC) by calling them on 1300 363 992; writing to them at GPO Box 5218 Sydney NSW 2001; emailing them at enquiries@oaic.gov.au or visiting their website at www.oaic.gov.au.

14. ANNEXURE A – Notifiable Data Breaches ('NDB') Policy

In 2017 the Notifiable Data Breaches ('NDB') scheme in Australia was established under Part IIIC of the Privacy Act 1988. The scheme was implemented on 22 February 2018. Under the scheme, a data breach must be reported if there has been an unauthorised disclosure or unauthorised access to Personal Information and the breach is likely to result in harm to one or more individuals. This is known as an Eligible Data Breach ('EDB').

The NDB scheme outlines requirements for Australian entities such as CSA in its response to data breaches. Should a data breach occur and is likely to result in 'serious harm' CSA must notify the Office of the Australian Information Commissioner ('OAIC') within 72 hours.

14.1 What is an Eligible Data Breach (EDB)?

An EDB arises when the following three criteria are satisfied:

- Data Breach – this occurs when there is unauthorised access to or unauthorised disclosure of personal data, or a loss of personal data that CSA holds.
- Serious Harm – the data breach is likely to result in serious harm to one or more individuals.
- Remedial Action – CSA has not been able to prevent the likely risk of serious harm with remedial action.

14.2 What is a Data Breach?

The first step to determine if an EDB has occurred involves considering whether there has been a Data Breach being:

- Unauthorised access to; or
- Unauthorised disclosure of personal data, or a loss of personal data.

The main categories of Data Breaches under the NDB scheme are described below:

Unauthorised access

This is where someone who is not permitted to have access has accessed Personal Information that CSA holds on your behalf. This includes unauthorised access by an employee of the CSI Group, or a Contractor as well as unauthorised access by an external third party (such as by hacking). The CSI Group has specific I.T. Security teams and controls to manage this..

Unauthorised disclosure

This occurs when CSA, (whether intentionally or unintentionally) makes your personal data accessible or visible to others outside of the CSI Group (e.g. if an employee of CSA accidentally publishes a confidential data file containing personal data of clients in an email).

Loss of personal data

This refers to the accidental or inadvertent loss of your personal data held by CSA/CSI group (E.g. if an employee of CSA leaves personal data, unsecured computer equipment, or portable storage devices containing our client's personal data on public transport).

14.3 Serious Harm

Whereas 'serious harm' is not defined in the Privacy Act 1988 in the context of a data breach, the OAIC have described it as any of the following:

- Serious physical, psychological, emotional, financial or reputational harm.

14.4 Types of Personal Data and Serious Harm

Some types of Personal Information may be more likely to cause an individual serious harm if compromised. Examples of the types of information that may increase the risk of serious harm if there is a data breach include:

- 'Sensitive information' such as details about an individual's health;
- Documents commonly used for fraud (e.g. Medicare card, driver licence, passport details);
- Financial information, such as credit card details.

14.5 Reporting a Data Breach

If CSA has reasonable grounds to believe it has experienced an EDB, it must promptly notify affected persons and the OIAC about the breach by submitting an Eligible Data Breach Statement within 72 hours.

The statement must include the following information:

- The date, or date range of the unauthorised access or disclosure
- The date CSA detected the data breach
- The circumstances of the data breach
- Who has obtained or is likely to have obtained access to the information
- Relevant information about the steps CSA has taken to contain or remediate the personal data breach

14.6 The OAIC Form for lodging Statements to the Commissioner

The OAIC has an on-line form for entities to lodge EDB statements under section 26WK of the Privacy Act 1988. The form is located at:

https://webform.oaic.gov.au/prod?entitytype=DBN&layoutcode=DataBreachWF

14.7 Notifying AUSTRAC or the Australian Cyber Security Centre of an EDB

The Australian Transaction Reports and Analysis Centre ("AUSTRAC") recommends that Reporting Entities (such as CSA) that encounter an EDB should, as a matter of good practice, inform AUSTRAC of the EDB or, if the breach involves a cyber-related incident, the Australian Cyber Security Centre ("ACSC").