

Privacy Policy

1 December 2024

Privacy Policy

1. Legislation

The *Privacy Act 1988* (Privacy Act) requires entities bound by the Australian Privacy Principles to have a privacy Policy. The Office of the Information Commissioner (OAI) is responsible for privacy functions that are conferred by the Privacy Act 1988.

2. What kinds of Personal information is collected and held?

Keystone Capital (Keystone) may be required to collect and hold personal information in order to provide services to our clients. Generally the kinds of personal information we may collect includes:

your name, home address, work address, email address, telephone number and signature.

When recruiting employees or appointing contractors Keystone may collect and hold personal information such as: the individual's name, contact details, date of birth, citizenship, employment references, civil credit and criminal records, regulatory accreditation (such as RG 146 accreditation for advisers) and driver's licence information, education and employment history. Once appointed we will also collect and hold TFNs, financial information relating to the appointing and banking details for payments.

3. How is it collected?

For our clients, personal information is mainly collected via meetings, telephone, email or correspondence and online forms.

4. Why we collect, hold, use and disclose clients' personal information?

Keystone collects, holds, uses and discloses clients' personal information for the purposes of:

- › providing financial products or services; and
- › complying with our regulatory or legal requirements, including:
 - the Anti-Money Laundering & Counter-Terrorism Act 2006
 - the Corporations Act 2001 the Australian Securities and Investments Commission Act 2001
 - the Bankruptcy Act 1966
 - the Tax Laws Amendment (Implementation of the FATCA Agreement) Act 2014
 - the Tax Laws Amendment (Implementation of the Common Reporting Standard) Act 2016; and
 - applicable taxation law.

5. How is it held?

We respect the personal information you have entrusted to us and we have a responsibility to manage and protect that information.

Your personal information will be stored in a secure environment in hard copy, electronically or both. With the exceptions detailed within this policy, your information will only be available to employees of Keystone or our service providers on a need-to-know basis in order to perform their obligations and duties.

6. What happens if personal information security is breached?

We implement corrective plans if our security measures are breached or your personal information is lost or inadvertently accessed by an unauthorised person. You and the Privacy Commissioner will be advised if we assess the data breach is likely to cause you serious harm.

7. How do you access your personal information and seek correction of it?

Should you wish to know what personal information Keystone holds on you, you may request to view this information by contacting our Privacy Officer:

Name: Keystone Privacy Officer

Address: Level 1, 265 Pirie Street Adelaide SA 5000

Tel no.: 08 7231 8777

Email: admin@keystonecapital.com.au

3

The Privacy Officer will promptly investigate your privacy enquiry and provide you with appropriate answers where required. Should you discover that any information is outdated, incorrect or incomplete you may request to have the personal information corrected and Keystone will promptly update our records. You may also contact the Privacy Officer if you have any questions on our compliance with the *Privacy Act 1988* (Cth).

8. How can I complain about a breach of my privacy?

If you wish to make a complaint about our handling of your personal information you should contact the Keystone Privacy Officer as referred to above. If we cannot resolve your complaint then you may raise your issue with the Office of the Australian Information Commissioner.

All privacy breaches that have resulted in or are likely to result in serious harm to any individual affected are 'eligible data breaches' which must be reported by Keystone to the Office of the Australian Information Commissioner.

9. To whom might it be disclosed

Generally Keystone will only disclose your personal information for the purposes of providing our financial products or services to you. This may include disclosing your personal information to related entities of Keystone and third parties where necessary to provide you with our financial products or services. These third parties may include government departments and regulatory authorities. They may also include our auditors, insurers, custodians, IT providers and third party administrators (service providers).

We may disclose personal information to overseas recipients in order to provide our financial products and/or services. Before disclosing any personal information to an overseas recipient Keystone will take reasonable steps to ensure the overseas recipient complies with the Australian Privacy Principles (AAPs) or is bound by a substantially similar privacy regime or you otherwise consent to the overseas disclosure or the disclosure is required or authorised by law.

10. Is sensitive personal information collected?

Keystone will not collect sensitive personal information on clients. Sensitive personal information is information 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 or biometric templates.

11. Notifiable Data Breaches

Keystone is required to notify individuals and the Office of the Australian Information Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- › there is unauthorised access to or disclosure of personal information held by us (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- › this is likely to result in serious harm to any of the individuals to whom the information relates.
- › we have been unable to prevent the likely risk of serious harm with remedial action

We will conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

12. Additional information

Further information on privacy in Australia may be obtained by visiting the website of the Office of the Australian Information Commissioner (OAIC) at: <http://www.oaic.gov.au/>. We regularly review the OAIC website to keep informed of issues and developments in privacy law and changing legal obligations.