



Mason Stevens Privacy Policy



Purpose

Mason Stevens Limited (ACN 141 447 207) (**'Mason Stevens'**, **'we'**, **'us'**, **'our'**) understands the importance and is committed to the protection and confidentiality of its clients' personal information.

Mason Stevens is bound by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (**APPs**) for the handling of personal information. Mason Stevens is also subject to Corporations Act 2001(Cth) (the **Act**) and Regulations and ASIC Regulatory Guides.

This Privacy Policy (**Policy**) outlines:

- The kinds of personal information that Mason Stevens collects and holds.
- How Mason Stevens collects and holds personal information.
- The purposes for which Mason Stevens collects, holds, uses and discloses personal information.
- Where Mason Stevens is likely to disclose personal information to overseas recipients and if practicable, the countries in which they are likely to be located.
- How Mason Stevens will assess a suspected data breach and report eligible data breaches.
- How you may access the personal information that Mason Stevens holds about you and seek correction of that information, and
- How you may complain about a breach of the APPs, including how your complaint will be dealt with.

Personal information we collect

"Personal information" is any information that identifies an individual or can be linked to an individual. The type of personal information that Mason Stevens collects includes; your name, contact details (such as your address, telephone number and email address), date of birth, tax file number (or tax identification number equivalent), gender, bank account and investment details.

Anti-Money Laundering and Counter Terrorism Financing Act 2006 (**AML/CTF Act**) and other applicable laws and regulations may also require us to collect additional personal information from you.

We collect personal information to enable us to provide you with our products and services.

How we collect personal information

Mason Stevens primarily collects personal information through its standard forms, such as an Application Form or through our investment and administration platform. We may further obtain information through telephone conversations, correspondence or direct contact.

Phone calls to some Mason Stevens employees may be monitored or recorded for training, regulatory or other compliance reason. We will advise you if this is the case.

In certain cases, we may collect personal information from third parties. For example, we may need to collect personal information from a representative (such as a legal adviser) or your financial adviser.

Website and platform

Mason Stevens will be aware of your identity only when you are logged into our platform using your login credentials.

The data we collect are statistical information on website and platform activity, such as the number of users who visit, the date and time of visits, the pages viewed and how users navigate through the website and platform and other anonymous information.

Information on visits to the website or platform are automatically collected. To collect this information, we may use session cookies. These cookies are used as a security measure to validate your identity before allowing you access to your confidential account information.

We collect this information for the purposes of our own analysis (and in these cases will only do so in aggregate form without identifying individual subscribers).

Using and disclosing personal information

The information we collect from you is strictly confidential for use within Mason Stevens. We use your personal information to establish and administer the financial products and services provided to you and to communicate with you on an on-going basis about those financial products and services.

Mason Stevens employees and its outsourced service providers (e.g. administrators) may use personal information to verify your identity over the telephone.

Unless you choose to opt out, Mason Stevens may also send you educational or marketing material about new products or services or other opportunities. You may contact us at any time and ask that we not send this material.

Mason Stevens may disclose personal information to external persons or entities, including regulatory authorities as described below:

- Mason Stevens may be required to provide details to a governmental or regulatory body to fulfil its legal requirements (for example, disclosure to enforcement bodies such as the Australian Securities and Investments Commission (**ASIC**), the Australian Taxation Office (**ATO**), the Australian Transaction Reports and Analysis Centre (**AUSTRAC**).
- In order to comply with the Foreign Account Tax Compliance Act (**FATCA**) and the Common Reporting Standard (**CRS**), Mason Stevens is required to collect certain information about your tax residency status. The ATO may pass this information onto tax authorities in other jurisdictions who have adopted FATCA and/or CRS.
- Mason Stevens may be required to disclose certain information pursuant to a court order.
- Mason Stevens uses agents and external service providers, (such as registry and administration providers, printing companies, external consultants) to assist it with the delivery of the financial products and services Mason Stevens provides to you.
- Mason Stevens will take steps to ensure that its agents and external service providers keep the personal information confidential, and that the information is only used for the purpose Mason Stevens has authorised. Those parties must undertake to comply with our confidentiality requirements under privacy law.

Where personal information is passed to external parties that perform specific services for Mason Stevens, Mason Stevens limit the disclosure to the information needed to perform the service. Depending upon the products or service you select, Mason Stevens may exchange information about you with, for example:

- other financial institutions, including stockbrokers, custodians and fund managers,
- insurance companies,
- superannuation funds,
- other organisations or firms, who jointly with us, provide products or services to you.

You may authorise Mason Stevens to disclose personal information we hold to your financial adviser or other person nominated by you. Your express consent is required prior to disclosure being made.

Mason Stevens will only disclose personal information where we are allowed to by law and have your express or implied consent, or where we are obliged to by law.

Mason Stevens may rely on some of the exemptions permitted in the Privacy Act, such as the exemption for disclosing information to a related body corporate.

Sending information overseas

Generally, Mason Stevens uses systems and services located within Australia. From time to time, we may send your information to recipients located overseas, including to related parties and service providers or other third parties who operate or hold data outside Australia. We may also send information overseas to complete a particular transaction or matter where this is required by the laws and regulations of Australia or another country.

Where your information is sent overseas, it is likely to be one of the following countries:

- Czech Republic;
- Hong Kong;
- India;
- Malaysia;
- New Zealand; and
- Singapore.

Where we send your information overseas, there are structures in place to ensure that appropriate data handling and security arrangements occur.

At times, clients may require Mason Stevens to send information to an overseas jurisdiction in order to facilitate a transaction. Mason Stevens endeavours to handle the outgoing information securely however is not responsible for any data loss or security breach once information has been received in that jurisdiction.

At times, your financial adviser may request outsourced third parties to operate as their office administrators. Mason Stevens reserves the right to refuse providing access to the outsourced third party, particularly where jurisdictions of third parties are located in high-risk jurisdictions, fail to demonstrate adequate data handling controls, or Masons Stevens has reason to believe sufficient notice has not been provided to the end client.

Notifiable Data Breach (NDB) Scheme

Mason Stevens has an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting your personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 established the NDB scheme in Australia (part IIIC of the Privacy Act 1988) which came into effect on the 22 February 2018. Under the scheme, Mason Stevens is required to notify particular individuals and the Office of the Australian Information Commissioner (**OAIC**) of any 'eligible data breaches'. An eligible data breach happens when:

- There is unauthorised access to or unauthorised disclosure of personal information, or loss of personal information, held by an entity; and
- The access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

'Serious harm' can be psychological, emotional, physical, reputational, financial or other forms of harm.

Suspected data breach

Mason Stevens is required to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information. All employees are required to inform the Privacy Officer immediately of any suspected data breach they become aware of. Data breaches include, but are not limited to:

- the unintended publication of personal or sensitive information; or
- the loss of an electronic device containing personal or sensitive information e.g. a phone, laptop or USB storage device; or
- email(s) sent to the wrong recipient containing personal or sensitive information; or
- unauthorised access to the Mason Stevens investment and administration platform.

Assessment

Mason Stevens will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If Mason Stevens has reasonable grounds to believe this is the case, then it must notify the OAIC. If Mason Stevens only has grounds to suspect this is the case, then it must conduct an assessment to determine if serious harm is likely.

The assessment should be conducted within 30 days and if this is not possible the reasons why should be documented.

Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in Mason Stevens' position. The Privacy Officer or their delegate will make the assessment.

Remedial action

Where possible, Mason Stevens should take steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is accessed or changing access controls on compromised client accounts before unauthorised access can occur.

If remedial action is successful in making serious harm no longer likely, then notification to the OAIC is not required.

Notification

Where serious harm is still likely (despite any remedial action taken), the Privacy Officer must prepare a statement for the OAIC (a form is available on their website). Mason Stevens must also notify affected individuals and inform them of the contents of the statement.

There are three options for notifying individuals:

- 1) Notify all individuals; or
- 2) Notify only those individuals at risk of serious harm; or
If neither of these options are practicable:
- 3) Publish the statement on the Mason Stevens website and publicise that the statement is available.

Mason Stevens may provide further information in its notification, such as an apology and an explanation of actions taken to rectify the breach.

Maintenance of accurate records

Mason Stevens aims to make sure that the personal information we collect, use or disclose is accurate, complete and up-to-date.

If Mason Stevens is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, we will take reasonable steps to correct it. If you believe your personal information is inaccurate, out-of-date, incomplete or irrelevant or misleading, you can contact us or submit a change of details form available from us or from your financial adviser. We will respond to your request within a reasonable period and not charge you for making the request.

Where available, you may have online platform access and can login and directly edit your details in the relevant section.

If we correct personal information about you that was previously disclosed to another APP entity, we will take reasonable steps to notify the other APP entity of the correction where that notification is requested by you.

Protecting your information and our website

The security of personal information is a priority for Mason Stevens, and we take reasonable steps to protect it from misuse, interference, loss, modification, unauthorised access or disclosure. We achieve this through the following measures.

Paper documents are protected from unauthorised access or use through the various security systems that are in place at our premises. We also maintain up-to-date computer and network security systems with appropriate firewalls, encryption technology and passwords to protect electronic copies of personal information.

Mason Stevens will take reasonable steps to destroy or permanently de-identify your personal information if it is no longer needed for any purpose for which the information may be used or disclosed in accordance with the APPs:

- if it is not contained in a Commonwealth record; and
- if we are not required by or under an Australian law, or a court / tribunal order, to retain the information.

Internet

To protect your personal information online, Mason Stevens uses secure technology methods.

For example, the Mason Stevens website has electronic security systems in place, including the use of firewalls and data encryption. User identifiers, passwords or other access codes may also be used to control access to your personal information.

However, you should be aware that the internet is not a totally secure environment. Mason Stevens cannot guarantee the security of information you provide to us if your chosen method is via the internet.

From time to time, we may provide access to external websites by clicking on links we have provided. Any external websites are not subject to our privacy standards, policies and procedures and therefore you are encouraged to review those websites to ascertain their privacy standards, policies and procedures before providing any of your personal information.

Access to your personal information

You may request access to the personal information we hold about you. This right of access is subject to some exceptions and where it is not possible to comply with your request, we will endeavour to explain why.

Contact us

If you have any questions about this Policy, concerns about a breach of the Australian Privacy Principles or you wish to make a complaint about how Mason Stevens has handled your personal information please contact our Privacy Officer.

Any complaint will be handled in accordance with our Complaints Handling and Dispute Resolution Policy brochure which is available on our website.

You can contact us by using one of the following methods:

Mail:	Privacy Officer Mason Stevens Level 26 420 George Street Sydney NSW 2000	Phone:	1300 988 878
		Email:	wealth@masonstevens.com.au