

PRIVACY POLICY

Source	<p>Privacy Act 1988, Regulations 2001, Privacy Amendment (Private Sector) Act 2000, the National Privacy Principles (NPP), Anti Money Laundering and Terrorism Financing Act 2006 (AML/CTF Act).</p>
Obligation	<p>The private sector provisions of the Privacy Act centre around 10 National Privacy Principles (the NPPs) that set out how private sector organisations should collect, use, keep secure and disclose personal information (refer Guideline 1 for a summary of the 10 NPPs). The NPPs give individuals a right to know what information an organisation holds about them and a right to correct that information if it is wrong.</p> <p>At Treasury Group Investment Services (TIS) the privacy of your personal information is important to us. When collecting, holding, using, disclosing personal information about an individual TIS must, in accordance with the NPPs, meet those standards. When collecting and handling personal information we aim to always promote the responsible collection and handling of an individuals' personal information by TIS and its employees, contractors and service providers (related and unrelated).</p> <p>With the commencement of the Anti-Money Laundering and Terrorist Financing Act (AML/CTF Act) in 2006 (Cth), TIS as a reporting entity under that Act, must also comply with the NPP if and when it collects, uses, stores and retains documentation containing personal information with regard to an individual.</p>
Application	<p>This policy applies to all TIS employees, any contractors and all authorised representatives, who may in the context of TIS carrying on a financial services business, be involved in the collection, use, disclosure and storage of an individual's personal information (customers and employees).</p>

Procedure

What is personal information?

Personal information means information or an opinion that allows others to identify an individual and includes an individual's name, age, gender, contact details as well as financial information relating to the individual.

Why TIS may collect personal information?

TIS may collect, store, use or disclose personal information obtained or provided to it by an individual for various reasons including:

- to provide you with the products and services you request as well as information about compatible or related products and services we offer;
- as a requirement under particular legislation (e.g. AML/CTF Act 2006) and report on compliance and risk management matters to regulators (e.g. ASIC, AUSTRAC) and our related bodies;
- to administer, monitor and evaluate products and services;
- to gather, aggregate and report statistical information;
- to assist you with any queries or complaints;
- to take measures to prevent or manage fraud and other legal activities (e.g. money laundering, financing of terror);
- to conduct the required background checks prior to hiring new staff members;
- to disclose to certain third party service providers who we outsource certain tasks. These third parties are bound by confidentiality agreements when handling your personal information and before we share your personal information with third parties, other than of this kind, without your consent;
- If you used a financial adviser who recommended your investment in the funds (as indicated on your application form), then details of your investments may be provided to your current financial adviser.

When collecting and handling an individual's personal information TIS will ensure the following general principles

are adhered to:

Collecting personal information

- Only collect personal information if it is necessary for your functions or activities.
- Use fair and lawful ways of collecting personal information.
- Take reasonable steps to ensure that the personal information you collect is complete and up to date. This may require you to correct the information.
- At the time that you collect personal information or as soon as practicable afterwards, take reasonable steps to make the individual aware of:
 - why you are collecting information about them; and
 - who else you might give it to

Dealing with personal information

When disclosing an individual's personal information with third parties other than external service providers including unit registry, mailing houses, information technology support and email suppliers, TIS must see an individual's consent before doing so.

We are committed to taking reasonable steps to protect the personal information you hold from misuse and loss and from unauthorised access, modification or disclosure. We will take reasonable steps to destroy or permanently de-identify personal information if we no longer need it for any purpose for which we may use or disclose the information.

Security

We are committed to ensuring that any personal information you provide to us remains confidential and secure. All our data is stored in written and/or electronic form and we maintain physical, electronic and procedural safeguards to protect your personal information.

We restrict access to information about clients to those employees, corporate partners and third party providers who need to know that information to deliver services and products efficiently and effectively.

Internet privacy

We receive information from browsers when you visit our website such as your server address, domain name, date and time of your visit, pages visited and selected information for statistical purposes only. No personal information is available on the TIS website. At the moment, TIS does not have a website.

Comment [NL1]: This is still the case for TIS is it not, TRG has a website?

Accuracy of your personal information

We aim to ensure that the personal information we retain about you is accurate, complete and up-to-date. You will be taken to agree to the use, collection and disclosure of your personal information when you make an investment in the fund. If you provide us with incomplete or inaccurate information, we may not be able to provide you with the products or services you are seeking or alternatively we may need to request for further information to be provided to us before we proceed in providing you with the products or services you are seeking.

Access and correction

We aim to give individuals a general right of access to their personal information and the right to have that information corrected if it is inaccurate, incomplete or out-of-date. An individual who wishes to access or correct their personal information should contact TIS's Privacy Officer by calling our Service Centre on (02) 8243 0400.

AML/CTF and Employee Due Diligence

As a reporting entity under AML/CTF Act TIS has certain obligations and in doing so it may need to disclose your personal information that it has obtained from you to RISQ, a third party provider of background checking for all new or prospective employees. When collecting personal information in the context of recruitment some points to consider:

- Personal information obtained during recruitment must not be disclosed.
- Resumes should only be viewed by those involved in the process.
- Only collect information that is needed to assess suitability for the role.
- Information must be collected directly from the candidate unless they consent otherwise.

Treasury Group Investment Services

Questions, complaints and requesting further information

If you have any questions, complaints or would like further information on our privacy and information handling practices, you can contact our Privacy Officer by calling our Service Centre on (02) 8243 0400.

Breaches

Any breach of this policy or any associated procedures must be **immediately** reported to TIS Risk and Compliance Services (RCS).

Monitoring

Management reporting and sign-off to Boards
Regular reviews by TIS RCS
Compliance checking by TIS RCS
Random spot checking by TIS RCS

Reports

Monthly/quarterly management reporting to Board and independent annual review by external Auditors

Amendments

This policy can be amended by the Managing Director and RCS is responsible for review, updating and communicating changes to the business as required.

GUIDELINE 1- National Privacy Principles (NPP)

The NPPs aim to ensure that organisations that hold information about people handle that information responsibly. They also give people some control over the way information about them is handled.

The following is a summary of the NPP, the full NPP can be found at Schedule 1 to Schedule 3 of the Privacy Act 1988.

NPP 1: Collection

Describes what an organisation should do when collecting personal information, including what they can collect, collecting from third parties and, generally, what they should tell individuals about the collection.

NPP 2: Use and Disclosure

Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are rules about direct marketing.

NPPs 3 & 4: Information quality and security

An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

NPP 5: Openness

An organisation must have a policy on how it manages personal information, and make it available to anyone who asks for it.

NPP 6: Access and Correction

Gives individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.

NPP 7: Identifiers

Generally prevents an organisation from adopting an Australian Government identifier for an individual (e.g. Medicare numbers) as its own.

NPP 8: Anonymity

Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves.

NPP 9: Transborder data flows

Outlines how organisations should protect personal information that they transfer outside Australia.

NPP 10: Sensitive information

Sensitive information includes information such as health, racial or ethnic background, or criminal record. Higher standards apply to the handling of sensitive information.