Privacy Policy & Procedure

Last Updated: May 2023

INTRODUCTION

The *Privacy Act 1988* (Cth) (**"Privacy Act"**), as amended by the Privacy Amendment (Enhancement Privacy Protection) Act 2012, establishes a scheme based on the Australian Privacy Principles, which regulates the collection, use, disclosure, handling, security, transfer and management of personal information, including electronically stored or transmitted information.

In order to comply with our privacy obligations you must:

- provide clients with a Privacy Statement prior to collecting personal information;
- provide access to our Privacy Policy;
- obtain client consent to collect, use and disclose their personal information;
- have procedures in place for access and correction of a client's personal information; and
- comply with the provisions of our Privacy Policy and the Privacy Act.

Under the FASEA Code of Ethics Standard 4 you have an obligation to ensure that before you act for the client you should consider explaining clearly (among other things) clearly and simply and ensuring the client understands and consents to the privacy and confidentiality arrangements applicable to them.

RESPONSIBILITY

This policy is the responsibility of the Responsible Managers.

REVIEW

This policy will be reviewed annually.

PROVIDING CLIENTS WITH A PRIVACY STATEMENT

Under the Privacy Act, you must notify persons of certain information about how you collect and disclose their information, prior to collection of this information. To satisfy this requirement, Pennywise Financial Services has incorporated a Privacy Statement within the FSG. You must provide a client with a copy of the FSG prior to collecting personal information from them in the course of providing financial services. This will also help you to meet your requirements under Standard 4 of the Code of Ethics.

Pennywise Financial Services has a documented Privacy Policy which outlines how we collect, use, disclose and manage client information. In addition to complying with the Privacy Act, you are required to be familiar with and comply with Pennywise Financial Service's Privacy Policy.

You are also required to direct the client to where they can obtain a copy of the Privacy Policy. Your FSG provides information on how a client can access the Privacy Policy.

Providing your client with an FSG will therefore meet your obligation to provide this information to the client.

UPDATES TO THE PRIVACY DOCUMENTS

Updating of the Privacy Policy and related documents is the responsibility of the Compliance Committee.

Access to Personal Information

Clients can request access to their personal information held on file, however, there are some instances where you may not be able to provide clients with access to this information.

We must give clients access to their personal information when they request it, and respond within a reasonable period and give them access in the manner they need.
If we refuse access to personal information, we must provide the reasons in writing and let the customer know how to complain about our refusal.

Security of personal information

We must take reasonable steps to protect the personal information we hold from misuse, interference, loss and from unauthorised access, modification or disclosure. This includes introducing measures to protect against computer attacks. We also need to take reasonable steps to destroy or de-identify personal information if it is no longer needed for any authorised purpose. The exception to this is where we are required to retain the information under Australian law or a court/tribunal order.

Adoption, use or disclosure of Government Identifiers

In order to comply with our privacy obligations, we must not use Tax File Numbers (TFNs), Medicare numbers or any other government identifiers as our own identifier. For example, we cannot use a customer's TFN to identify a customer in our records.
When collecting information that contains a TFN (eg a tax assessment notice) you must receive consent to maintain the TFN (eg via the TFN Authorisation in the Fact Find or the TFN Consent form. If you do not have consent you must black out/ delete/destroy the TFN at the time the information is collected.

When do I need to obtain consent from clients in relation to their personal information?

The Privacy Act requires that you only use and disclose a client's personal information in specific circumstances, such as where you have the client's consent or where you are required by law to do so (for example in response to a valid request for information from a government agency such as the ATO). You must collect information from the individual, ensure they have consented to collection of this information, only collect information reasonably needed for, or directly related to, one of our functions or activities. You must also not collect sensitive information unless the client consents to the collection and the sensitive information is reasonably necessary for one of our functions or activities.
Examples of sensitive information include:

- race or ethnic origin
- political opinions, membership of a political association
- religious beliefs or affiliations and philosophical beliefs
- membership of a professional or trade association or membership of a trade union
- sexual preferences and practices
- criminal record
- health information and biometric information including disability, illness (including HIV or AIDS), pregnancy.

Generally, we only collect sensitive information if it is necessary to provide customers with a specific product or service and they have consented to that collection. For example, we may collect health information to process a claim under an insurance policy or collect voice biometric information to verify identity or authorise transactions.

The Pennywise Financial Services Fact Find allows for a client to give their consent for obtaining, using and disclosing their personal information for the purposes of providing financial services. This is incorporated in the Client Declaration section of the Fact Find.

The Pennywise Financial Services Engagement Letter allows for a client to give their consent for obtaining and using and disclosing their personal information for the purposes of providing financial planning advice services.

In addition, Pennywise Financial Services has created a separate TFN Consent Form for use where a data collection form has previously been completed and no TFN consent was collected at that time. Refer to the Tax File Number (TFN) Policy for more information in relation to obligations relating to disclosing and storing TFN's.
You must ensure that a client has signed and dated the Client Declaration section of the Fact Find (or the TFN Consent form) in order to confirm their consent to use their personal information in line with our Privacy Policy.

What do I do if I receive unsolicited personal information?

An individual may provide us with unsolicited information i.e. information which we did not solicit.

If you receive unsolicited information you need to determine if it is reasonably needed for, or directly related to, one of our functions or activities. For example, is it required for the purposed of providing financial services or products to the client? If it is not, then you should destroy, de-identify or return to the client this information as soon as practicable, but only if lawful and reasonable to do so, and only if the information is not public knowledge.

What if I need to collect information from a third party?

Where you need to collect information about a client from a third party (e.g. a superannuation provider), you will need to make the client aware that you are going to do so, or have done so. This is achieved by ensuring that the client completes and signs the 'Client Authorisation for Additional Information from Other Institutions or Financial Advisers" Form.

What must not be kept on a client file?

Any personal medical information or other sensitive information which is not directly associated with your advice must be destroyed after the business has been written or declined by the underwriter, unless required to be maintained by law.
If you recorded this information in the Fact Find, or any other data collection document, it must be removed by scoring out the information.

If you recorded this information electronically, it must be deleted after the business has been written or declined.

Overseas Use of Data

Although we don't send personal information overseas you should be aware of the following:

- we take reasonable steps to ensure your information remains secure;
- your personal information may be accessed by our contractors, representatives or agents in other countries, if that becomes necessary to deliver our services to you. This access is via secure internet connection or, in some instances by email;
- from time to time, information may be loaded to the cloud for storage or access through programs such as drobox etc; and
- it is possible that suppliers we deal with may outsource functions using overseas contractors or companies that process these services using offshore resources. Where this is a concern to you, we suggest that you carefully read their privacy policy to determine the extent to which they send information overseas. These service providers have committed to adhering to the Australian Privacy Principles and the Privacy Act (1988).