

# Information Collection and Storage Policy

## Aim

The collection, handling and storage of client's Personal and Sensitive Information is regulated under the Privacy Act 1988 and the Australian Privacy Principles.

The policy aims to assist Advisers to understand.

- [What the differences are between Personal and Sensitive information](#)
- [The treatment of an Individuals Tax File Number](#)
- [How to handle request to release information to clients and third party](#)
- [Record keeping requirements in relation to personal and sensitive client information.](#)

This policy does not address the record keeping requirements in relation to the client files. Please refer to the Maintaining client file policy for additional guidance.

## Background

The *Privacy Act 1988* (Privacy Act) is an Australian law which regulates the handling of Personal Information about individuals. This includes the collection, use, disclosure and storage of Personal Information, and access to and correction of that information.

The Privacy Act also contains provisions that deal with the collection, security and disposal of individuals' Tax File Numbers, credit information and health or medical information.

The Licensee has adopted the principles set out in the Privacy Act and the Licensee's Privacy Policy

## Definitions

**Australian Privacy Principles:** There are 13 privacy principles that regulate the handling of Personal Information.

**De-identification:** For the purposes of privacy, de-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. This may involve removing personal identifiers such as name, address, date of birth and Tax File Numbers; or removing or altering other information that may allow an individual to be identified due to rare characteristics.

The de-identification of personal Information will prevent others from misusing it.

**Financial Service:** means the provision of financial products or advice such as life insurance, superannuation and retirement income, managed investments and financial planning services and financial product advice.

**Personal Information:** This includes 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. The Personal Information may include a person's name and address, medical records, bank account details, photos, videos and even information about what an individual likes, their opinions and where they work.

**Personal Information Security:** Means keeping Personal Information secure from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

**Sensitive Information:** Sensitive Information has the meaning as set out in s 6(1) of the Privacy Act and includes information or an opinion about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, criminal record, health information and some aspects of genetic and biometric information.

**Tax File Number Information:** means information that connects a TFN with the identity of a particular individual (for example, a database record that links a person's name and date of birth with the person's TFN).

## Requirements

The client's Personal Information (including content which may be sensitive) will generally be collected in a number of ways – for instance during the Fact Find, obtained upon the receipt of financial statements, documented within file notes, and often saved electronically within financial planning software.

The collection, use, disclosure, and storage of a client's Personal Information is required to be handled carefully as a contravention of the Privacy Act carries civil penalty orders of up to \$340,000 for individuals and up to \$1.7 million for companies.

For this reason, it is important that you observe the requirements of this policy when handling any Personal or Sensitive Information you collect about your clients.

### Personal and Sensitive Information

You may only collect Personal and Sensitive Information about a client where the:

- Information is needed to provide advice or implement a product.
- Information is required by law or
- The client has consented to provide you with this information.

Personal Information you may hold about a client may include the name, address, gender, marital status, contact details and date of birth; occupation and employer details; details of the Financial Service the client applied for, and details of any financial products purchased or invested in (including account details); and for insurance products, certain medical, family and lifestyle information.

The collection, use, disclosure, and storage of Sensitive Information generally requires a higher level of privacy protection.

If you collect Personal and Sensitive Information about a client you must take reasonable steps to protect the information from misuse, interference, and loss, as well as unauthorised access, modification or disclosure. You are required to notify a client (or clients) and the Office of the Australian Information Commissioner (OAIC) if an 'eligible data breach' occurs in relation to their personal information that is held by you. A data breach may occur if personal information is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference.



#### **Obtaining Client Consent**

**The client must consent for you to use the information collected for the purpose of providing the client with financial products and services. Unless this consent is given, you cannot, by law, retain the information on file.**

### Recording tax file numbers

Where the client provides consent, you are permitted to retain the client's TFN on file. If you do not have a signed Client Consent, you are required to de-identify (or remove) the TFN from the file immediately.

TFNs are treated as Sensitive Information and must therefore be always kept confidential. You are required to have safeguards in place to prevent the unauthorised access and use of this information.

### Rights to remain anonymous.

Under the Privacy Act, a potential client may choose to remain anonymous in their initial dealings with you. In such situations you are required to explain to the client that to effectively provide financial advice, the client will be required to disclose all relevant details about themselves.

Under the Anti Money Laundering and Counter Terrorism Financing Act (AML/CTF), you will however be prevented from providing a financial service until such time as the client has been identified. Should the client refuse to provide such identification, you must decline to provide financial advice to them.

## Client Access and Correction of Information

Clients (or their appointed representative) have the right to access or check the Personal Information held about them.

Requests for access to limited amounts of Personal Information, such as checking to see what address or telephone number we have recorded, can generally be handled in person or over the telephone – only after you have appropriately verified their identity.

If the request relates to updating information that is no longer accurate, you must take reasonable steps to correct the information so that it remains accurate and up to date.

### Dealing with requests to access the client file.

Under the Privacy Act, you are required, on request, to give clients access to the Personal Information you hold about them unless an exception applies (see the 'Exception to the Rule' on the next page).



#### Exception to the Rule

Not all Personal Information should be made available to the client. The Australian Privacy Principle 'Access to, and correction of, personal information' states that you are not required to give the client access to Personal Information where:

- Giving access would pose a serious threat to the life, health or safety of the client.
- The request for access is frivolous or vexatious.
- The information relates to existing or anticipated legal proceedings.
- Giving access would have an unreasonable impact on the privacy of other individuals (for instance in the case of separation / pending divorce).

## Releasing client information to third parties

Client information must not be passed onto third parties unless the client has provided written authority to do so. Obtaining the client's consent provides the authorisation to communicate clients' Personal Information to external parties including:

- Third parties (e.g. under a court order) may also be provided access to client's Personal Information and
- Other professionals such as accountants, solicitors and stockbrokers when a referral is required.

Requests from Austrac and the Australian Tax Office do not require client consent.

## Personal Information Security and Storage

Client's Personal Information must always be kept secure and protected from misuse, loss, unauthorised access, modification and disclosure.

The Privacy Principles require that you can retain Personal Information for as long as you need it to provide the Financial Services requested by the client and, in some circumstances, to comply with statutory requirements. The information you maintain must be securely stored for 7 years. After this time you are required to destroy it if you have not obtained the client's consent to continue to maintain it; or if there is a risk of the information being accessed by an unauthorised third party. Client consent is taken to include their consent to continue to receive advice or service from an adviser.

The following 5 principles are 'guiding principles' only and are not mandated, however they may assist in determining how best to manage the destruction of Personal (or Sensitive) Information that is no longer required.

1. Any printed document that contains Personal Information must only be disposed of by either shredding or placement in a secure document destruction bin.

2. Any electronic storage devices such as CDs, DVDs, memory sticks, USBs etc that contain Personal Information must be wiped clean of data and then disposed of by placement in a secure document destruction bin.
3. Where boxes of files or documents are archived or destroyed, a list of their content and their archive or destruction date should be maintained.
4. In circumstances where documents or electronic records exist and may be relevant to a current or reasonably anticipated claim, complaint, legal action or regulatory issue, such documents or electronic records must not be deleted or destroyed.
5. All client files or documents containing Personal or Sensitive Information must be stored in a secure location at the end of each business day.

Please refer to the **Maintaining Client Files** policy for the client file and record retention processes.

## Additional Licensee Requirements

### How must I document client consent to collect and store information?

FPQ must be completed, Authorisation forms and filed on PRP's approved software program.

### How must I provide clients with the Licensee's Privacy Policy?

The Licensee's Privacy policy must be placed on all website/s.

### What steps should I take if I receive a request for a copy of a client file?

You must always obtain specific consent from the client to disclose his/her Personal Information.

### What information can we share with relatives of a deceased client?

Disclosure of Personal Information is related to 'living persons' by law. However as an Adviser, you should take into consideration your duty of confidentiality to the deceased client. You must be mindful of the legal implications you may face if you disclose the information to the 'wrong' person, especially where family disputes may arise.

### What information can we share with the spouse (where both members of a couple are clients)?

You must always obtain specific consent from the client to disclose his/her Personal Information to the spouse.

## Penalties

Failure to adhere to the Licensee's Compliance policies, industry bodies' Codes of Conduct to which you are a member, and the law may result in further supervision, training, disciplinary action, banning/deregistration, fines, and ancillary orders of restitution to effected clients' as well as possible criminal penalties.

## Tools

- Licensee's Privacy policy
- Fact Find or Review Fact Find
- Standalone Privacy Acknowledgement and Consent (CWT only)

## Resources

Privacy Act 1988

Australian Privacy Principles