Version –July 2021

# PRIVACY POLICY

# Table of Contents



# VERSION

| Date | Changes |
|---|---|
| Feb 2021 | Policy reviewed. |
| Jul 2021 | Amended the policy to:<br>• Encompass the 4 key elements relating to a client's consent.<br>• Include reference to item 6 of the TPB's Code of Professional Conduct.<br>• Require a client's informed consent prior to providing the client's information overseas. |
| | |

# POLICY

## Purpose

AFD[1] understands that the privacy of client information is important and we respect the confidentiality of the information that is provide to us. Protecting a client's information is an important part of maintaining trust between us and our clients and by handling information in a secure manner we build strong business relationships.

This document provides information and details about how we manage the personal information that we collect, hold, use and disclose about individuals.

This Privacy Policy applies not only to us as holder of an Australian Financial Services License ("The Licensee") but also to each of our Authorised Representatives. As such, reference to **AFD, us, we or our** also includes reference to each Adviser who has been appointed as an Authorised Representative of AFD.

Please note, if an Adviser also provides Credit Services, those services are not covered by us and that Adviser will need to liaise with their Credit Licensee's Privacy Policy.

AFD is bound by the Privacy Act and personal information is managed in accordance with the Australian Privacy Principles. AFD and its Authorised Representatives are also required to comply with the Code of Professional Conduct, as administered by the Tax Practitioners Board (TPB), and the Code of Ethics, as administered by the Financial Adviser Standards and Ethics Authority (FASEA).

We may amend or update our Privacy Policy as required by law or as our business processes or technology changes. When we do, we will post the updated policy on our website – www.ausfindir.com.au. We encourage you to check our website from time to time to view our current policy or contact us for a printed copy.

## Definitions

For the purposes of this document, the following are defined as:

**Consent** means express consent or implied consent and must address the following 4 key elements:

- the individual is adequately informed before giving consent – consequences of not consenting must be disclosed to the individual;
- the individual gives consent voluntarily – consent cannot be bundled together with multiple requests without giving the individual an opportunity to choose which privacy clauses they agree to;
- the consent is current and specific; and
- the individual has the capacity to understand and communicate their consent.

**Eligible data breach** arises when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information in circumstances where unauthorised access is likely to occur;
- a reasonable person would conclude that the unauthorised access, disclosure or loss would likely result in serious harm to any of the individuals to whom the information relates; and
- AFD has not been able to prevent the likely risk of serious harm with remedial action.

**Personal information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

**Sensitive information** means:

(a) information or an opinion about an individual's:
  i. racial or ethnic origin; or
  ii. political opinions; or
  iii. membership of a political association; or
  iv. religious beliefs or affiliations; or
  v. philosophical beliefs; or

[1] AFD holds an Australian Financial Services Licence AFSL 344971 and is a "professional" licensee. AFD's Authorised Representatives operate their own practice and provide financial services to their own clients.

vi. membership of a professional or trade association; or
vii. membership of a trade union; or
viii. criminal record;

(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information; or
(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) biometric templates.

**Serious harm** is not defined in the Privacy Act 1988. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

## Collection and use of personal information

AFD collects, holds, uses and discloses personal information so as to provide financial services to clients.

The collection and use of personal information may also be required for the following purposes:

- Complying with our legal obligations, such as verifying a client's identity;
- Assisting with clients with questions and complaints;
- Arranging for services to be provided by third parties;
- Internal operations, such as record keeping, data analytics, auditing or training; or
- Promotion of other products and services that may be of interest to clients.

Please note that, for the purposes of this policy, the Financial Services being provided by an Adviser do not include Credit Services.

The collection and use of personal information may sometimes be disclosed to other people with whom we do business (including employees) in order to administer and manage our business operations. This information is afforded the same standard of care as that of our clients.

## Protection of personal information

We strive to ensure that the personal information provided to us is stored safely and securely. We take a number of precautions to protect the collected personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

We have a range of practices and policies in place to protect personal information we hold, including:

- educating our staff and representatives about how to protect personal information and updating them about cybersecurity developments, threats and scams;
- requiring our staff and representatives to use passwords when accessing our systems;
- where appropriate, using strict confidentiality arrangements restricting third parties' use or disclose of personal information for any unauthorised purposes;
- employing physical and electronic means, including access controls (as required) to protect against unauthorised access to buildings;
- employing firewalls, intrusion prevention systems and virus scanning tools to protect against unauthorised persons, malware and viruses from entering our systems;
- some of the systems we use are on dedicated secure networks or transmit electronic data via encryption; and
- providing secure storage for physical records and securing paper files in locked cabinets and physical access restrictions.

Where personal information is no longer required, we take steps to de-identify or destroy the information in a secure manner.

## What personal information is collected

We ask people for a range of personal information to assist us in providing relevant products and services. The information we collect could include (but is not limited to) a client's name, date of birth, contact details, financial information, employment details, residency and citizenship status. We may also collect the personal information of a client's family members where it is relevant to the advice being provided.

We may also collect sensitive information about a client's medical history and their health and lifestyle to provide financial advice about life insurance products.

In most instances, we collect personal information directly from that person when they:

- complete a financial product application form,
- complete an identification form,
- complete data collection documentation,
- interact with an online interactive tool, such as a budget planner,
- provide documentation to us, or
- when a client communicates with us in person, over the telephone, fax, email, internet or by using other electronic devices.

Situations where we collect personal information from other people and organisations include (but are not limited to):

- a financial adviser,
- other professionals who act on your behalf, such as a lawyer or accountant,
- health professionals,
- other organisations, who jointly with us, provide products or services to you, and
- social media and publicly available sites.

It's a client's choice whether or not to provide personal information to us. However, in this case, the adviser must warn the client about the possible consequences of their decision and how this may impact on the quality of the advice provided.

The adviser may also decline to provide advice if they feel they have insufficient information to proceed. In some instances, we will decline to provide services or advice if we feel we have insufficient information for the scope of the service or advice requested.

Further, in some circumstances the law requires us to obtain and verify details of photographic and non-photographic identification documents.

## Notification of eligible data breaches

AFD will notify the Commissioner and affected individuals of an eligible data breach, which is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in AFD's position.

## Cookies and the use of other web technologies

Some personal information may be collected automatically, i.e. without a client's knowledge, whilst navigating through and interacting with the content of our websites. The electronic methods of collection used include cookies, log files and web beacons.

Cookies log files and web beacons are usually small text, log or pixel file stored on a device that records information when visiting our websites. They are used to improve a client's website experience, to provide relevant information and to manage a client's access to certain parts of our websites. Changing a client's browser settings may limit access to some parts of our websites.

## Accessing and updating personal information

A client can request access to their personal information. There may be a justifiable cost involved with locating, copying or sending the requested information. If applicable, the cost is to be discussed and agreed with client.

There may be circumstances where the requested information is commercially sensitive and it would be inappropriate to provide it. In these situations, the client is to be informed and an explanation provided.

Any request for access to personal information is to be actioned as soon as possible with the aim being to respond within five (5) working days. The timeframe is subject to the complexity of the type of information requested.

A client may wish to remain anonymous or to use a pseudonym when dealing with us. In such circumstances client's must be advised that the information or services may be limited or may not be possible to be delivered.

# Sharing of personal information

A client's personal information may be shared with other entities both within and outside of the Licensee.

This will vary according to the product or service involved, but could include:

- any person acting on a client's behalf, including financial adviser, solicitor, accountant, executor, administrator, trustee, guardian or attorney etc;
- financial product and service providers, including financial planning software providers and paraplanners;
- for corporate superannuation members, your employer or your employer's financial adviser;
- other organisations within the Licensee including related bodies corporate and advice firms;
- medical practitioners and health service providers, such as pathology services;
- companies involved in the payments system including financial institutions, merchants and payment organisations;
- organisations who assist with certain business functions, such as auditors, compliance consultants, direct marketing, debt recovery and information & communication technology support;
- our solicitors, our insurers, courts, tribunals or dispute resolution organisations;
- other organisations who provide us with products & services so that they may provide their products & services to you or contact you on our behalf, and/or
- anyone to whom we, or our service providers, are required or authorised by law to disclose your personal information to (for example, law enforcement agencies, Australian and international government or regulatory authorities).

Subject to compliance with Item 6 of the TPB's Code of Professional Conduct, information may also be disclosed to a third party, where consent has been provided, or where a client would reasonably expect us to disclose your information to that third party. Information may also be provided to financial advisers, companies and consultants that we work with. The only circumstances in which personal information would be used or disclosed would be if we are required or authorised by law to do so.

Personal information collected may also be used for direct marketing purposes to promote events, products or services that may be of relevance to a client, however, the client must be given the opportunity to opt out of this form of communication.

# Disclosure of personal information overseas

There may be instances when a client's personal information may need to be disclosed to overseas service providers. If a client's personal information is to be provided to overseas third parties, the client must provide their informed consent before the client's personal information is provided to an overseas their party. Advisers must not advise the client that appropriate data handling & security arrangements are in place until the client has given their informed consent.

# Complaints about privacy

Privacy complaints/queries are to be directed to AFD's Privacy Officer who will provide a response to the complainant within 30 days. The Privacy Officer's contact details are:

**Mail:** Australian Financial Directions Pty Ltd
Level 1, 197 Adelaide Tce, East Perth WA 6004
PO Box 6222 East Perth WA 6892

**Phone:** (08) 6556 2992

**Email:** afd@ausfindir.com.au

**Web:** www.ausfindir.com.au

If a client is not fully satisfied with our response, they are entitled to contact the Office of the Australian Information Commissioner ("OAIC"). The OAIC's contact details are:

**Mail** GPO box 5218 Sydney NSW 2001

**Phone** 1300 363 992

**Email** enquiries@oaic.gov.au

**Web:** www.oaic.gov.au

Ω