AUSTRALIAN ADVICE NETWORK

Privacy Policy and Collection Statement – Australian Advice Network

AFSL: 472901
Last Updated: 4th June 2025
Version: 5

Privacy Policy and Collection Statement (Privacy Policy)

1. Introduction

Australian Advice Network Pty Ltd (referred to as AAN, ***we***, ***our***, ***us***) is bound by the *Privacy Act 1988* (***Privacy Act***), including the Australian Privacy Principles (***APPs***), and recognises the importance of ensuring the confidentiality and security of your personal information.

This document provides information and details about how we manage the personal information that we collect, hold, use and disclose about individuals. The Privacy Policy applies to all organisations within the Licensee and any subsidiary companies.

All third parties (including clients, suppliers, sub-contractors, or agents) that have access to or use personal information collected and held by AAN, must abide by this Privacy Policy and Collection Statement (**Privacy Policy**). AAN makes this Privacy Policy available free of charge and can be downloaded from its website www.australianadvicenetwork.com.au.

In this Privacy Policy:

- ***Disclosure*** of information means providing information to persons outside of AAN;
- ***Personal information*** means information or an opinion relating to an individual, which can be used to identify that individual;
- ***Privacy Officer*** means the contact person within AAN for questions or complaints regarding AAN's handling of personal information;
- ***Sensitive information*** is personal information that includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences and criminal record, and also includes health information; and
- ***Use*** of information means use of information within AAN.

2. Why we collect and use personal information

We collect, hold, use and disclose personal information so we can provide you with financial advice, services and products, advice and service relevant to your needs. We may also collect, use and disclose your information for related purposes such as:

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

3. What kind of personal information do we collect and hold?

We may collect and hold a range of personal information about you to provide you with our services, including:

- name;
- address;
- phone numbers;
- email addresses;
- occupation;
- bank account details;
- residency and citizenship status;
- driver's licence (or other identification) details;
- financial information, including details of:
    - your investments;
    - your insurance policies;
    - your superannuation/pension policies;
    - estate planning strategies;
    - Centrelink payments;
    - taxation information; and
    - health information.

4. How do we collect personal information?

We generally collect personal information directly from you. For example, personal information will be collected through our application processes, forms and other interactions with you in the course of providing you with our products and services, including when you visit our website, use a mobile app from us, call us or send us correspondence.

We may also collect personal information about you from a third party, such as electronic verification services, referrers and marketing agencies. If so, we will take reasonable steps to ensure that you are made aware of this Privacy Policy.

We will not collect sensitive information about you without your consent, unless an exemption in the APPs applies. These exceptions include if the collection is required or authorised by law, or necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct.

It's your choice whether to provide your personal information. You have the right not to provide personal information, including about your identity. However, in this case, your adviser will warn you about the possible consequences and how this may impact on the quality of the advice provided. Your 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.

We do not give you the option of dealing with us anonymously, or under a pseudonym. This is because it is impractical, and, in some circumstances, illegal for AAN to deal with individuals who are not identified.

5. Unsolicited personal information

We may receive unsolicited personal information about you. We destroy or de-identify all unsolicited personal information we receive, unless it is relevant to our purposes for collecting personal information. We may retain additional information we receive about you if it is combined with other information we are required or entitled to collect. If we do this, we will retain the information in the same way we hold your other personal information.

6. Who do we collect personal information about?

The personal information we may collect and hold includes (but is not limited to) personal information about:

- clients;
- potential clients;
- service providers or suppliers;
- a financial adviser;
- a mortgage broker or credit representative;
- health professionals;
- prospective employees, employees and contractors; and
- other third parties with whom we come into contact for example solicitors or accountants.

This information is afforded the same standard of care as that of our clients.

7. Website collection

We collect personal information when we receive completed online generated forms from our website www.australianadvicenetwork.com.au. We may also use third parties to analyse traffic at that website, which may involve the use of cookies. Information collected through such analysis is anonymous.

To use our website, you must consent to our use of cookies. You can withdraw or modify your consent to our use of cookies at any time. If you no longer wish to receive cookies, you can use your web browser settings to accept, refuse and delete cookies. To do this, follow the instructions provided by your browser. Please note that if you set your browser to refuse cookies, you may not be able to use our website and/or all of the features of our website.

Cookies do not contain personal information in themselves but can be used to identify a person when combined with other information. Cookies are small text files which are transferred to your computer's hard drive through your web browser that enables our website to recognise your browser and capture and remember certain information.

8. Why do we collect and hold personal information?

We may use and disclose the information we collect about you for the following purposes:

- provide you with our products and services;
- review and meet your ongoing needs;
- provide you with information we believe may be relevant or of interest to you;
- let you know about other products or services we offer, send you information about special offers or invite you to events;
- consider any concerns or complaints you may have;
- comply with relevant laws, regulations and other legal obligations; and
- help us improve the products and services offered to our customers and enhance our overall business.

We may use and disclose your personal information for any of these purposes. We may also use and disclose your personal information for secondary purposes which are related to the primary purposes set out above, or in other circumstances authorised by the Privacy Act.

Sensitive information will be used and disclosed only for the purpose for which it was provided (or a directly related secondary purpose), unless you agree otherwise, or an exemption in the Privacy Act applies.

By law, we are required to comply with record keeping obligations such as keeping records for at least seven years after advice has been provided to you, and Customer Identification Procedure records for the duration of your relationship with your adviser and for an additional seven years after you stop receiving any designated services.

9. Who might we disclose personal information to?

We may disclose your information to a third party where you have given your consent or where you would reasonably expect us to disclose your information to that third party. We may disclose personal information to:

- a related entity of AAN;
- an agent, contractor or service provider we engage to carry out our functions and activities, such as our lawyers, accountants, auditors, compliance consultants, debt collectors, IT support or other advisers;
- organisations involved in a transfer or sale of all or part of our assets or business;
- organisations involved in managing payments, collecting fees, including payment merchants and other financial institutions, such as banks;
- regulatory bodies, government agencies, law enforcement bodies and courts;
- financial product issuers;
- for corporate superannuation members, your employer or your employer's financial adviser;
- a person acting on your behalf such as a power of attorney, executor, administrator, trustee or guardian;
- financial planning software providers and external paraplanners;
- lenders and other credit providers;
- medical practitioners and health service providers, such as pathology services; and
- anyone else to whom you authorise us to disclose it or is required by law.

If we disclose your personal information to service providers that perform business activities for us, they may only use your personal information for the specific purpose for which we supply it. We will ensure that all contractual arrangements with third parties adequately address privacy issues, and we will make third parties aware of this Privacy Policy.

The only circumstances in which we would collect, use or disclose your government related identifiers is where we are required or authorised by law to do so. For example, we may be required to disclose your Tax File Number (TFN) to the Australian Taxation Office, a superannuation or retirement income product provider. Likewise, we may need to disclose your Medicare number to Centrelink in order to assess your social security eligibility. Drivers licence numbers and passport numbers may also be collected when we are required to verify your identity.

10. Sending information overseas

AAN, nor the advisers within AAN, do not currently engage in any third-party service providers that assist in the provision of products or services that are based overseas. Your adviser will notify you if this was to change in the future.

If AAN were to use offshore providers, we will not send personal information to recipients outside of Australia unless:

- we have taken reasonable steps to ensure that the recipient does not breach the Act and the APPs,
- the recipient is subject to an information privacy scheme similar to the Privacy Act; or
- the individual has consented to the disclosure.

If you consent to your personal information being disclosed to an overseas recipient, and the recipient breaches the APPs, we will not be accountable for that breach under the Privacy Act, and you will not be able to seek redress under the Privacy Act.

11. Management of personal information

We recognise the importance of securing the personal information of our customers. We will take steps to ensure your personal information is protected from misuse, interference or loss, and unauthorised access, modification or disclosure.

Your personal information is generally stored in our computer database. If any paper files are maintained they are stored in secure areas. We have a range of practices and policies in place to protect personal information we hold, including:

- Compulsory use of passwords and two-factor authentication are required to access the system, and passwords are routinely checked;
- Compulsory secure password management software to be used to record passwords. Passwords are not permitted to be written down or shared to another person via email;
- all computers which contain personal information are secured both physically and electronically;
- Encrypting personal information if it is to be released to a third party;
- educating our staff and representatives about how to protect your personal information and updating them about cybersecurity developments, threats and scams;
- where appropriate, using strict confidentiality arrangements restricting third parties' use or disclose of personal information for any unauthorised purposes;
- data and cyber security assessments of third-party providers and systems;
- Implementation of the Australian Cyber Security Centre Essential 8;
- 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;
- Annual reviews of our practices cyber security systems;
- Retaining documents required by law for the statutory period (e.g. 7 years for some transaction data under AML/CTF law), but de-identifying it and restricting access after this time;
- a Cybersecurity policy, Cyber Incident Response Plan and Data Breach Response plan in place; and
- some of the systems we use are on dedicated secure networks or transmit electronic data via encryption.

Where our employees work remotely or from home, we implement the following additional security measures:

- two-factor authentication is enabled for all remote working arrangements;
- password complexity is enforced and only secure Wi-Fi is permitted to be used;

- we ensure that employees only have access to personal information which is directly relevant to their duties;
- employees must ensure that no other member of their household uses their work device;
- employees must store devices in a safe location when not in use;
- employees may not make hard copies of documents containing personal information, nor may they email documents containing personal information to their personal email accounts;
- employees must follow the Work From Home Policy; and
- employees may not disclose an individual's personal information to colleagues or third parties via personal chat groups.

12. Direct marketing

We may only use personal information we collect from you for the purposes of direct marketing without your consent if:

- the personal information does not include sensitive information; and
- you would reasonably expect us to use or disclose the information for the purpose of direct marketing; and
- we provide a simple way of opting out of direct marketing; and
- you have not requested to opt out of receiving direct marketing from us.

If we collect personal information about you from a third party, we will only use that information for the purposes of direct marketing if you have consented (or it is impracticable to obtain your consent), and we will provide a simple means by which you can easily request not to receive direct marketing communications from us. We will draw your attention to the fact you may make such a request in our direct marketing communications.

You have the right to request us not to use or disclose your personal information for the purposes of direct marketing, or for the purposes of facilitating direct marketing by other organisations. We must give effect to the request within a reasonable period of time. You may also request that we provide you with the source of their information. If such a request is made, we must notify you of the source of the information free of charge within a reasonable period of time.

13. Identifiers

We do not adopt identifiers assigned by the Government (such as drivers' licence numbers) for our own file recording purposes, unless one of the exemptions in the Privacy Act applies.

14. How do we keep personal information accurate and up to date?

We are committed to ensuring that the personal information we collect, use and disclose is relevant, accurate, complete and up to date.

We encourage you to contact us to update any personal information we hold about you. If we correct information that has previously been disclosed to another entity, we will notify the other entity within a reasonable period of the correction. Where we are satisfied information is inaccurate, we will take reasonable steps to correct the information within 30 days, unless you agree otherwise. We do not charge you for correcting the information.

15. Accessing your personal information

Subject to the exceptions set out in the Privacy Act, you may gain access to the personal information that we hold about you by contacting the AAN's Privacy Officer. We will provide access within 7 (seven) business days of the individual's request. The time however to provide this information will depend on the type of information requested and if it is expected that it will take longer than 7 days, this will be discussed with you.

There may be circumstances where we refuse to provide you with the information you request, for example when the information is commercially sensitive. In these situations, we will inform you and provide an explanation as to why.

We will require identity verification and specification of what information is required. There may be a cost involved with locating, copying or sending you the information you request. The cost will be discussed and agreed with you at the time.

16. Incidents/Complaints handling/Making a complaint

We have an effective complaint handling process in place to manage privacy risks and issues.

The complaints handling process involves:

- identifying (and addressing) any systemic/ongoing compliance problems;
- increasing consumer confidence in our privacy procedures; and
- helping to build and preserve our reputation and business.

You can make a complaint to us about the treatment or handling of your personal information by lodging a complaint with the Privacy Officer.

If you have any questions about this Privacy Policy, or wish to make a complaint about how we have handled your personal information, you can lodge a complaint with us by contacting the Privacy Officer on the information below:

Mail	PO Box 7045, GCMC, QLD, 9726
Phone	07 5551 0855
Email	info@australianadvicenetwork.com.au
Website	www.australianadvicenetwork.com.au

We will acknowledge receipt of a complaint immediately, however, where this is not possible, acknowledgement will be made as soon as practicable. We will then investigate the complaint and respond to you within 30 days. Some complex matters may require an extension to thoroughly investigate the complaint and bring it to resolution.

If you are not satisfied with our response to your complaint, you can also refer your complaint to the Office of the Australian Information Commissioner by:

- telephoning – 1300 363 992
- writing – Director of Complaints, Office of the Australian Information Commissioner, GPO Box 5218, SYDNEY NSW 2001
- email – enquiries@oaic.gov.au
- online submission – https://forms.business.gov.au/smartforms/landing.htm?formCode=APC_PC

You may also direct privacy complaints related to financial advice to:

The Australian Financial Complaints Authority (AFCA). AFCA provides fair and independent financial services complaint resolution that is free to consumers. Their contact details are:

- **Mail** GPO Box 3, MELBOURNE VIC 3001
- **Phone** 1800 931 678 (free of charge)
- **Email** info@afca.org.au
- **Online** **www.afca.org.au**

17. Contractual arrangements with third parties

We ensure that all contractual arrangements with third parties adequately address privacy issues, and we make third parties aware of this Privacy Policy.

Third parties will be required to implement policies in relation to the management of your personal information in accordance with *the Privacy Act*. These policies include:

- regulating the collection, use and disclosure of personal and sensitive information;
- de-identifying personal and sensitive information wherever possible;
- ensuring that personal and sensitive information is kept securely, with access to it only by authorised employees or agents of the third parties; and
- ensuring that the personal and sensitive information is only disclosed to organisations which are approved by us.