Privacy Policy

Overview

Professional Wealth Services Pty Ltd (PWS) (**Licensee**) adheres to the Australian Privacy Principles (**APPs**) and is committed to protecting your privacy. The purpose of this Privacy Policy is to outline how we collect, use, disclose and retain personal and sensitive information. It also sets out how you can make a complaint and how you can access the personal information we hold about you.
Our business is to help you understand and achieve your financial goals.
To do this, we need to understand who you are, what you want to achieve and what your circumstances are. We therefore need to collect personal information about you. This is so we can determine what services you require and what products suit your needs. We collect, use, retain and disclose your personal information so we can help you achieve your goals and at the same time operate our business and meet the legal and regulatory requirements.
We may also use and disclose your information for purposes related to those mentioned above, such as:

- assisting with your questions and complaints;
- arranging for services to be provided by third parties; and
- record keeping, compliance training and auditing.

This privacy policy is reviewed annually (unless an update is required earlier).

What is personal information?

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not. For the purposes of this policy, personal information may include:

- Name;
- Address;
- Nationality;
- Residency status;
- E-mail address;
- Tax File Number; and
- Financial information.

Collection of personal information

Collection of personal information

We may collect and hold personal information for the purposes of enabling us to provide financial services to you. For example, in order for us to provide personal advice to you, we are required to verify your identity and obtain information relating to your financial situation and your personal goals and objectives – this is so we can assess your personal situation and provide you with appropriate financial advice. This information is generally collected directly from you as our client.
Any personal information collected by us is solely for the purpose of providing services to its clients and will not be disclosed unless the disclosure is required in the performance of those services (for example, disclosing your information to a financial institution in order to place an investment on your behalf). Where we obtain sensitive information (e.g. racial or ethnic origin, political opinions, religious beliefs or affiliations or criminal record), we will only do so with your consent and where the collection of such information is reasonably necessary for us to perform our function. For example, we may also collect sensitive information (e.g. your health records) for the purposes of arranging insurance for you or assisting you with insurance claims.
We will only collect personal information by lawful and fair means. In general, we collect personal information about you from you unless you consent to the collection of your personal information from someone else or it is unreasonable or impracticable to do so. In some instances, we may collect this information through third parties such as your family members, people authorised by you or health professionals (e.g. in the case of income protection insurance).
Any personal information held by us may be held in a number of ways including via hard copy, soft copy or offsite on electronic servers. For example, we may collect personal information from you when you complete our client data form for the purposes of allowing us to provide you with financial advice or we assist you to acquire or dispose of a financial product (e.g. invest in a managed fund or rollover your superannuation).

Dealing with unsolicited personal information

If we receive unsolicited personal information, we will within a reasonable period after receiving the information, determine whether or not we could have collected the information under Australian Privacy Principle 3. If the information could not have been obtained under APP 3 we will take steps to destroy or de-

identify the information as soon as practicable, if it is lawful and reasonable to do so.

Notification of the collection of personal information

At or before the time we collect personal information about you, or if that is not practicable, as soon as practicable after, we will take reasonable steps to ensure you are aware of:

- who we are and our details;
- how we collect your personal information and whom from;
- whether the collection of your personal information is required or authorised by or under an Australian law or a court/tribunal order;
- the purposes for which we collect your personal information;
- the main consequences (if any) if we do not collect all or some of the personal information;
- any other person or body to whom we would disclose the personal information that we have collected;
- information about how you may access the personal information held by us about you and how you may seek correction of such information;
- how you may complain about a breach of the Australian Privacy Principles and how the entity will deal with such a complaint;
- whether we are likely to disclose the personal information to overseas recipients (if so where).

Anonymity and pseudonymity

You may wish to deal with us anonymously; however, this is likely to limit the services we provide to you as our principal business relates to the provision of financial services (and in most cases, the provision of personal advice) which would require individuals to provide personal information. We are also required under Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) to conduct customer due diligence and appropriately identify clients.

If you don't provide us with the information we request

It is your choice as to whether you wish to provide us with the information we request. However, given the nature of our business, we may not be able to provide you with the financial services you require if you don't provide us with the relevant personal information to help us review your personal circumstances.

Use or disclosure of personal information

If we collect personal information for a specific purpose (e.g. to provide financial services to you), we will not use or disclose the information for another purpose unless you consent to the use or disclosure of the information or an exception in the APPs applies.

Direct Marketing

We may use and disclose your personal information to keep you informed about the range of financial products and services that we think may be relevant or of interest to you. You can opt out of receiving direct marketing information from us at any time by contacting us.

Disclosure of information overseas

From time to time, we may send your information overseas to our service providers or other third parties who operate or hold data outside Australia. Where we do this, we make sure that appropriate data handling and security arrangements are in place. We will also advise you of the countries where your data may be stored.

Security and access to your personal information

Information accuracy

We take reasonable steps to ensure that all personal data collected is accurate, up to date and complete. You can ask us to correct any inaccurate information we hold or have provided to others by contacting us using the details in this policy. If the information that is corrected is information we have provided to others, you can ask us to notify them of the correction.

Security of personal information

We take care to protect the security of your personal information. We may hold your personal information in a combination of secure computer storage facilities, paper-based files and other formats. Professional Wealth Services Pty Ltd (PWS) uses a number of external service providers who have access to our client's data to help deliver our services to you such as insurers, external compliance providers, client management system (CMS) providers and electronic document signing facilities. Therefore, client personal information may be stored on servers hosted in Australia, but accessed by staff of these providers who are located in for example, the Philippines. We take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or improper disclosure, and conduct due diligence on these providers.

Please note, we are required by law to retain your personal information for a specific amount of time. We will generally destroy or de-identify personal information if it is no longer required.

Access to and correction of personal information

You can contact us to access or correct any personal information we hold about you. However, in certain situations, we are permitted to refuse access to personal information. These situations include where:

- giving access would have an unreasonable impact on the privacy of other individuals
- giving access would be unlawful, or where denying access is required or authorised by an Australian law or a court order
- giving access is likely to interfere with law enforcement activities.

For other situations, please consider Australian Privacy Principle 12.

If we receive a request to access personal information, we aim to respond to that request in a reasonable timeframe. In general, we will not impose an access charge unless the request of access and correct personal information is excessively onerous.

If we refuse access to personal information, we will provide you with reasons as to why access was refused and provide you with information on how to lodge a complaint about the refusal.

Data breach

A data breach occurs when personal information held by us is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing personal information of clients is lost or stolen, or when a database containing personal information is hacked or if we mistakenly provide personal information to the wrong person.

Under the Privacy Amendment (Notifiable Data Breaches) Act 2017, we have an obligation to assess within 30 days whether a data breach amounts to an 'eligible data breach' if we become aware that there are reasonable grounds to suspect that data breach may have occurred.

If we form the view that the data breach would likely result in serious harm to any of the individuals to whom the information relates despite any remedial action taken by us, then the data breach will constitute an 'eligible data breach'. If an eligible data breach occurs, we have an obligation to notify you and the Office of the Australian Information Commissioner and of the details of the eligible data breach.

Privacy Act Reforms

As part of the Privacy Act Reforms (**the Reforms**) there are a number of new legal obligations which raise the bar on how Australian businesses handle personal information and this includes the Licensee and its representatives.

The Licensee acknowledges that it can be sued for a serious breach of privacy and has satisfied itself that it has taken reasonable steps to ensure it protects the information it holds about its clients including the following:

- Auditing its data collection and storage practices;
- Implementing stronger cybersecurity protections;
- Provided training to staff on privacy risks, doxxing laws, and breach response;
- Reviewing contracts with suppliers and service providers who handle data;
- Updated its Data Breach Response Plan to reflect timely notification under the *Notifiable Data Breaches* (**NDB**) scheme; and
- Updated its risk management and controls.

Enhanced Consent

As part of this policy the Licensee acknowledges that consent with this policy by its clients must be voluntary, informed, current, specific, unambiguous and easily withdrawn. The Licensee can provide this policy to our clients in a number of ways, for example, referring clients to our website, emailing the policy to our clients or including the policy in other documents, for example our financial services guide.

Right to be forgotten

The Licensee acknowledges that clients should be informed of their right to be forgotten, specifically that they can request the deletion of their personal data when the data is no longer necessary for the purposes of which it was collected, and consent has been withdrawn, or the data was not lawfully collected. The Licensee must balance this right out with the record keeping obligation on the AFSL which includes keeping advice documents and materials used to produce advice for a minimum of 7 years as per ASIC Pro Forma 209.

Transparency in Automated Decision Making

Automated decision-making (**ADM**) involves using data, machines, and algorithms to make decisions across various contexts such as public administration, business, health, education, law, employment, transport, media, and entertainment. If the Licensee uses ADM, it will notify its clients accordingly as well as the significance and potential consequences for individuals.

Overseas Data Transfers

Where the licensee transfers data overseas and discloses personal information to overseas recipients, the Licensee will spell out the countries where recipients are located. The Licensee has taken measures to ensure these recipients comply with the Australian Privacy Principles (APPs and inform individuals of their rights concerning overseas disclosures). The

steps the Licensee has taken from a due diligence perspective are captured in the outsourcing risk register controls.
The Licensee currently transfers data to Asia Pacific.

Data Security Measures

The Licensee has implemented the following steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure:

- Regular staff training and discussion of incidents at team meetings.
- Adopted a Data Breach Response Plan.
- Regular testing and review of the Data Breach Response Plan.
- Due diligence of third-party providers who hold our client data.
- Adoption and regular review of systems and frameworks to protect cloud applications and devices from data breaches.
- Employs staff and engages outsourced providers with specialised expertise or experience in data breach prevention and response or engaging a consultant with appropriate expertise to assist with the development of it's a data breach response prevention and response.
- Adoption of a risk assessment and framework to identify, measure and treat data breaches.

Notifiable Data Breaches (NDB) Scheme

- The Licensee has procedures in place for detecting and responding to data breaches including a Data Breach Response Plan which provides examples of data breaches and what is reportable and what is not as part of its Data Breach Response Plan.
- The Data Breach Response Kit sets out a process for notifying affected individuals and the Office of the Australian Information Commissioner (OAIC) when a breach is likely to result in serious harm including the required timeframes.
- Timeframes for notification and remedial actions are included in the Data Breach Response Plan.

Individual Rights

The Licensee acknowledges that individuals have certain rights under the Privacy Act and the amended changes which commenced in June 2025. Part of these changes include:

- Having access to their personal information, specifically the information that the Licensee holds on its clients.
- Correcting inaccuracies in relation to the information that the Licensee holds on its clients.
- Requesting data deletion by clients and former clients in relation to information that the Licensee holds on its clients and former clients which it no longer requires.
- Acknowledging and respecting a client (or former client) may object to certain data processing activities.
- Acknowledging and respecting a client (or a former client) has a right to lodge a complaint with the OAIC.
- The right to sue for a serious breach of privacy as a result of the mishandling of data, even if the OAIC is not involved.

Children's Online Privacy

The Licensee's services are not directed at children and therefore the Licensee is not bound by the Children's Online Privacy Code. The Children's Online Privacy Code will be developed and registered by 10 December 2026.

Doxxing

The Licensee acknowledges that doxxing is now a serious offence and that publishing someone's private information, such as their address, work address and phone number with the intent to cause harm is now a criminal offence, even if it was accidental. This includes sharing information via social media. The Licensee has taken steps to train it staff about the dangers of doxxing and how it can put the Licensee's business at risk.

Contact us

You may wish to contact us for the following:

- find out what personal information we hold about you;
- update or correct the personal information we hold about you;
- Request we delete the data we hold about you
- opt out of receiving direct marketing material
- make a privacy related complaint with us of the Office of the Australian Information Commissioner (OAIC) .

Should you wish to do so, please contact us on the details below:

Professional Wealth Services Pty Ltd (PWS)
Level 12
141 Walker Street
North Sydney NSW 2059
AUSTRALIA

PO Box 1815
North Sydney NSW 2059
AUSTRALIA

Phone: 1300 001 312
Website: www.pws.net.au