Privacy Policy

Praemium Limited

Review:	Every 2 years (next due May 2026, unless required earlier)
Document Owner:	Chief Risk Officer (CRO)
Classification:	Internal Use Only

Approved by:

- Praemium Limited (PPS) 24 May 2024
- Praemium Australia Limited AFSL 297456 (PAL) 27 May 2024
- PowerWrap Limited AFSL 329829 (PWL) 27 May 2024
- MWH Capital Pty Ltd AFSL 338141 (MWH) 27 May 2024
- OneVue Wealth Services Ltd AFSL 308868 (OVWS) 27 May 2024
- Investment Gateway Ltd AFSL 239117 (IG) 27 May 2024
- OneVue Wealth Assets Ltd (OVWA) 27 May 2024

Contents

1. Overview

1.1 Background

This Privacy Policy (this **Policy**) applies to Praemium Limited (**PPS**) (ABN 74 098 405 826) and its subsidiaries and related entities (**Praemium, we us, our**). Praemium includes Praemium Australia Limited (**PAL**) (ABN 92 117 611 784), Powerwrap Limited (**PWL**) (ABN 67 129 756 850), MWH Capital Pty Ltd (**MWH**) (ABN 64 136 888 956), OneVue Wealth Services Ltd (**OVWS**) (ABN 70 120 380 627), Investment Gateway Ltd (**IG**) (ABN 91 090 411 537), and OneVue Wealth Assets Ltd (**OVWA**) (ABN 44 670 987 434).

1.2 Purpose

Praemium is required by the *Privacy Act 1988* (Cth) (**Privacy Act**) to have a privacy policy. This Policy sets out the requirements and guidelines for the protection of personal information of our clients, members, beneficiaries, and other individuals whose information we may collect and use. It sets out the:

- Legal and regulatory obligations to protect personal and sensitive information;
- Management of personal information including collection, use, disclosure, and security;
- Types of incidents that contravene and constitute a breach of privacy laws; and
- Process to respond in the event of a breach of privacy.

Praemium is required to publish this Policy on the Praemium website and make it available upon request. Section 1 of this Policy serves as an internal preamble to the Policy. Section 2 of this Policy onwards will be published to Praemium's website and may be periodically updated, as required, outside of the typical Board and Committee approval process. Any updates will be notified to the Boards and Committees as soon as practicable.

1.3 Scope

This Policy applies to all Praemium directors and employees, including contractors of Praemium (unless otherwise stated, hereafter referred to as "**employees**"). All employees are expected to understand the key principles, processes, roles, and responsibilities contained in this Policy.

1.4 Non-compliance

Any non-compliance with and breach of this Policy by Praemium employees will be taken seriously. In assessing non-compliance, each matter will be considered on a case-by-case basis according to its merits. Considerations may include the level and impact of non-compliance, reasons for non-compliance (e.g. training, human error, process failure, etc.), frequency and any other relevant circumstances.

1.5 Roles and responsibilities

Role	Responsibility
All staff	All staff have a responsibility to comply with the Privacy Act. All staff are expected to immediately report any privacy incidents, breaches, and complaints. Incidents and breaches should be reported via Azure DevOps or directly to the Risk & Compliance team. Privacy complaints should be brought to the immediate attention of the Complaints Handling Officer, as well as the Privacy Officer.

All managers	Responsible for ensuring that their staff understand their privacy obligations and that they immediately report any privacy incidents, breaches or complaints as required under this Policy.
Complaints Handling Officer	Responsible for managing privacy complaints in accordance with Praemium's Complaints Handling Policy.[1]
Privacy Officer	Responsible for Praemium's privacy compliance, assisting the business in managing privacy obligations, and having oversight of privacy incidents, breaches, and complaints.[2]

1.6 Definitions

Term	Definition
Personal information	Defined in the Privacy Act as 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. Common examples include: • An individual's name, , signature, address, telephone number or date of birth; • Financial information, such as bank account numbers and identifying numbers (i.e. numbers that are linked to a record owned by a person or entity); and • Identification documents.
Privacy complaint	An expression of dissatisfaction concerning privacy made to or about an organisation, related to its products, services, staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.
Privacy incident and breach	An incident or breach that involves privacy concerns. Note: An incident is where the end result of a process, function or action is not what was expected or is incorrect. A breach is a violation of, or failure to comply with, the law, AFSL conditions, a Scheme's Constitution or Compliance Plan or internal policies.
Sensitive information	Sensitive information is a type of personal information that includes information or an opinion about an individual's: • Racial or ethnic origin; • Political opinions or associations; • Religious or philosophical beliefs; • Trade union membership or associations; • Sexual orientation or practices; • Criminal record; • Health or genetic information; and • Some aspects of biometric information.

[1] The Complaints Handling Officer typically sits in the Client Experience team at Praemium.
[2] The Privacy Officer typically sits in the Risk & Compliance team at Praemium.

2. Privacy Policy

1. Praemium Privacy Policy

This Privacy Policy (this **Policy**) applies to Praemium Limited (**PPS**) (ABN 74 098 405 826) and its subsidiaries and related entities (**Praemium, we us, our**). Praemium includes Praemium Australia Limited (**PAL**) (ABN 92 117 611 784), Powerwrap Limited (**PWL**) (ABN 67 129 756 850), MWH Capital Pty Ltd (**MWH**) (ABN 64 136 888 956), OneVue Wealth Services Ltd (**OVWS**) (ABN 70 120 380 627), Investment Gateway Ltd (**IG**) (ABN 91 090 411 537), and OneVue Wealth Assets Ltd (**OVWA**) (ABN 44 670 987 434).

Your privacy is important to us. This Policy is aligned with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**). It sets out the key points about how Praemium may collect, use, and manage personal information.

This Policy is published on Praemium's website (https://www.praemium.com) and will be updated periodically and may be done so without notice. You should regularly review this Policy.

Please contact us if you would like to receive a copy of this Policy free of charge.

1.1 About Praemium

Praemium provides financial services, online portfolio administration and Customer Relationship Management (CRM) services to our customers, who are individuals and intermediaries such as financial advisers, accountants, stockbrokers and investment or superannuation administrators.

The Praemium services and products include:

- OneVue IDPS: an investor directed portfolio service;
- OneVue Managed Account: a managed investment scheme;
- OneVue Portfolio Administration Service: a non-custodial platform and portfolio administration service;
- Powerwrap Investment Account: an IDPS-like managed investment scheme;
- Separately Managed Accounts: a managed investment scheme;
- SuperSMA: Praemium acts as the sponsor of a superannuation fund;
- Virtual Managed Accounts/Virtual Managed Accounts Administration Service: a non-custodial platform and portfolio administration service; and
- YourChoice Super: Praemium acts as the sponsor of a superannuation fund.

Praemium may collect, hold, use and disclose personal information in operating its website and in providing its products and services to you.

2. Collection of personal information

2.1 Type of personal information collected

The products or services that Praemium provides you will determine what information we will collect about you. We will collect the following information when you:

- Contact us by phone, email or letter – name, date of birth, and contact details such as telephone numbers, email or postal address.

- Use of our website or social media – date and time of visit, pages viewed, the type of operating system used, your internet protocol (IP) address, the location of your server, the address of any referring website and whether any information has been downloaded.
    - See section 2.3 of this Policy for more information on our use of cookies.

- Participate in marketing activities – name, contact details such as telephone numbers, email or postal address, and employment status.

- Apply to use Praemium products or service – name, date of birth, signature, contact details such as telephone numbers, email or postal address, identification documents, tax and financial information, employment status, nominated beneficiaries, citizenship/residency status, and information derived from name screening checks.

- Apply to offer Praemium products or services to clients (e.g. as an AFS licensee or adviser) – name, date of birth, signature, contact details such as telephone numbers, email or postal address, bank details, details of your business such as licences and authorisations, and information derived from checks through ASIC and other such organisations.

- Apply to work at Praemium – name, date of birth, signature, contact details such as telephone numbers, email or postal address, bank details, superannuation and tax information, employment history, personal information about referees, and emergency contacts.

Praemium may collect or hold government-related identifiers (GRI) such as TFN, driver's licence, or passports to provide its products and services. Praemium is permitted to use or disclose a GRI for an individual if we believe that it is necessary for one or more enforcement-related activities conducted by or on behalf of a body such as ASIC, AUSTRAC or the Australian Federal Police.

Praemium is required to obtain consent before collecting sensitive information – see Section 2.4 of this Policy for more information.

2.2 How we collect personal information

Praemium collects personal information through a variety of methods and contact points during its business. We may collect information directly from individuals, or from other sources. In most cases, the information we collect is provided by you or by your financial adviser.

The method of collection will vary based on your relationship with Praemium, but includes the following:

- When you contact us or login to your account and make changes to your personal information, or upload information or documents into Praemium systems;

- When your financial adviser, or another authorised representative, logs in to your account and makes changes to your personal information, or uploads information or documents into Praemium systems;

- When you apply for a product or service with us, or your financial adviser does so on your behalf;

- When you use our website or social media;

- When you participate in marketing activities; and

- When you apply to work at Praemium.

Praemium may also collect personal information from other third-parties, including:

- Third-party product issuers, where Praemium administers those products;

    - You should consult these issuers' privacy policies to determine how they manage your personal information.

- When you apply to work at Praemium, we may perform a number of pre-employment due diligence checks (e.g. police, employment references, and bankruptcy);

- Regulatory and government bodies, such as the Australian Securities and Investments Commission, the Australian Taxation Office, and law enforcement agencies; and

- Other commercial service providers that enable us to provide our products and services and comply with the law, such as services which enable us to verify your identity and other information you have provided.

Where we request personal information from you, we will tell you why we are collecting it, how it will be used, and how we will manage and share your information. If you choose not to provide the requested information, we will inform you of the consequences of doing so (e.g. we may not be able to provide a product or service to you) – see Section 2.5 of this Policy for more information.

2.3 Collection of information through Praemium's website and use of cookies

Information may be collected through your use of Praemium's website, which enables us to tailor your online experience. The type of information that may be collected is non-personal information and will generally include information as outlined in section 2.1 of this Policy.

Although this information is non-personal, it may constitute personal information if when collated with other information that Praemium holds, it can be used to identify you. In this case the information will be treated in accordance with this Policy.

This information is collected through the identification of cookies that are stored on your device when you access and interact with Praemium's website. Notwithstanding the above, no attempt will be made by Praemium to identify you or your browsing activities, except where required under the law.

Visitors to Praemium's website can disable cookies through their internet browser. However, disabling cookies may limit the functionality of Praemium's website.

2.4 Sensitive information

This type of information is subject to more stringent obligations under the Privacy Act. Praemium does not generally collect sensitive information, but if we need this type of information Praemium will:

- Request (and receive) your prior consent;

- Only do so where it is necessary to collect the information for one or more of our functions and activities or to provide our products and services (and we will describe what this function is); or

- Only do so where it is required by or authorised under an Australian law or a court/tribunal order.

2.5 Anonymity and not providing requested information

The Privacy Act permits you to remain anonymous or use a pseudonym in certain dealings with Praemium. For example, you may choose not to provide your name or contact details when enquiring about a Praemium service or product. However, this option will generally not be available when you wish to use a Praemium product or service as we are required by law to establish the identity of anyone doing so.

You may also choose not to provide Praemium with certain pieces information that we have requested. If you do so:

- You may be prevented from using our products or services, or you may not be able to access a third-party product or service administered by Praemium;

- We may not be able to process your requests or instructions in a timely manner, or at all; or
- There may be financial implications (e.g. tax treatment or delays in processing market sensitive instructions).

2.6 Unsolicited information

There may be instances where Praemium comes into possession of personal information that it has not requested. For example, we may receive information from your adviser that we did not specifically request, such as health information related to insurance you hold.

If this occurs, Praemium may record or use this information if it could have collected this information through its ordinary course of business. A determination must be made promptly to determine whether the information could have been collected. If it is determined that the information would not have been collected through the ordinary course of business, it may need to be destroyed or de-identified.

Praemium's Privacy Officer has responsibility for reaching a determination and ensuring that unsolicited personal information is handled appropriately.

3. Use of personal information

3.1 How we use personal information

Praemium collects, holds or uses personal information for the purpose of providing its products and services and to comply with legal obligations such as those under superannuation law, taxation law and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). For example, Praemium may use clients' personal information to:

- Assess applications for our managed funds or other Praemium products;
- Adequately administer, invest, or transfer managed investments and/or superannuation benefits in Praemium products; and
- Enable Praemium to assist its clients with related services, as may be required from time to time.

Under the AML/CTF Act, Praemium is required to collect and verify (through identification documents such as a passport or driver's licence) its clients' names, addresses, and dates of birth. If clients do not provide Praemium with all or part of the information requested, we may not be able to provide the products or services in question.

3.2 Praemium marketing activities

Praemium does not in the ordinary course of business market directly to clients of advisers. Where we do engage in marketing activities, we will only do so where the:

- Information used to contact the person was collected by Praemium, and not by another third-party;
- Person would reasonably expect Praemium to contact them for marketing purposes; and
- Person has not opted out of any marketing communications from Praemium.

In any instance where personal information is collected from a person, Praemium must seek their consent to the receipt of marketing activities. All marketing activities will contain a prominent option for individuals to opt out. Where an opt-out from receiving marketing material is received this will be recorded, appropriate systems updated, and this preference stored with that person's personal information details.

In undertaking marketing activities, Praemium complies with obligations in relation to the following:

- The *Do Not Call Register Act 2006* (Cth) and *Do Not Call Register (Consequential Amendments) Act 2006* (Cth); and

- The *Spam Act 2003* (Cth), which prohibits the sending of unsolicited commercial electronic messages - known as spam - with an Australian link.

3.3 Disclosure to third parties

The disclosure of personal information at times involves its release to third parties, including entities within the Praemium group. Disclosure includes providing other companies with electronic access to records, transferring physical records to someone else's possession, or discussing the personal information of a client with external persons.

The Privacy Act generally prohibits the disclosure of personal information to third parties unless the following exceptions apply:

- The individual affected has provided consent to the disclosure;

- The disclosure of the information is related to the purpose for which it was collected;

- It is required by law, or an order of an Australian court or tribunal; or

- Exceptional circumstances apply, such as an imminent risk to health or of criminal activity.

Praemium may provide personal information in accordance with the exceptions listed above, including to a:

- Third-party broker to execute a trade on a client's portfolio;

- Trustee(s) of the products and services provided by Praemium;

- Third parties who provide administration services to Praemium;

- Investment managers or other financial institutions to facilitate or manage an investment (including cash); and

- Insurers, underwriters, or medical practitioners for life insurance purposes or for determining superannuation benefits.

3.4 Cross border disclosure

Some of the software systems that Praemium uses involve personal information being transferred to and held in data centres in jurisdictions outside of Australia. We may disclose your information to related overseas entities for the purpose of providing internal support for our service and product offerings.

In addition, we may disclose certain information where the disclosure is required or permitted by law. For example, the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) requires Praemium to collect and provide information about foreign investors who have investments in our products. This information is lodged with the Australian Taxation Office which may ultimately pass it on to the US Government's Internal Revenue Service or the relevant foreign taxation authorities.

Where you or your adviser instruct us to invest in international assets or administer international non-custodial assets, we may be required to share your personal information with overseas recipients. We will take reasonable steps to ensure that overseas recipients do not breach the APPs, or the overseas recipients are subject to laws which protect personal information in a way which is comparable to the protection provided by the APPs. However, Praemium is not responsible for, and cannot be held liable for, how these overseas recipients use your personal information.

4. Management of personal information

4.1 Protecting personal information

Personal information that is collected by Praemium may be stored electronically or in hard copy form. It may be held directly by Praemium or a service provider who Praemium has engaged to provide such services.

Praemium has implemented processes and systems to ensure personal information is protected and used only for the purposes for which it was collected. Some of the measures we have in place include:

- All transmitted data is encrypted on secure networks;
- Firewalls, intrusion detection systems and anti-malware/anti-virus tools are in place;
- Physical security measures are in place, including cameras and smartcards;
- Database access is controlled, and third-party agreements reflect privacy obligations;
- Internal access to client records and databases is restricted based on employee roles and responsibilities;
- Authorisation processes are in place for changes in access;
- User access management is in place across Information Technology systems;
- Client records in hard copy format are secured and archived where appropriate; and
- Employee education including training, policies and procedures (including clean desk).

Note, however, that Praemium cannot be responsible for user access that an adviser or other third parties may permit or manage.

Praemium has policies and processes in place for managing the retention of personal information. In most cases personal information will be retained for seven years after the cessation of Praemium's dealings with you.

In cases where Praemium is no longer required to maintain and hold records or personal information reasonable steps will be taken to de-identify or securely destroy this information.

4.2 Maintaining accurate records

It is important that Praemium ensures the personal information it collects is accurate, up-to-date and complete.

Accordingly, Praemium employees responsible for collecting or maintaining personal information, are appropriately trained to verify the accuracy of personal information (for example, through identity checks). In addition, procedures are in place to:

- Train client-facing and operational employees to ensure critical personal information is complete and correct;
- Record information consistently through standardised forms and data entry processes;
- Check data to minimise errors, such as peer-checking of data entries; and
- Provide options for clients or investors to update their personal information, including online portals or dedicated contact details.

We have created appropriate system access for your adviser to keep your personal information accurate and up to date. For certain Praemium products, your adviser may also grant you access to update your data.

There may be occasions when Praemium becomes aware that the personal information it holds is incorrect or out of date. When this occurs, Praemium must correct the records as soon as possible. It must take reasonable steps to do so, which could include:

- Contacting your adviser (or you in some circumstances) and verifying that the information is accurate, up-to-date and complete;
- Checking other available records to crossmatch information, such as public records or other records retained by Praemium (Note: TFNs cannot be used to crossmatch information – see Section 4.3 of this Policy); or
- Correcting the information it holds by re-entering data or altering its records.

4.3 Tax File Numbers (TFN)

There are legally binding guidelines relating to the collection, storage, use, disclosure, security, and disposal of individuals' TFN under the Privacy Act, the *Taxation Administration Act 1953* (Cth), the *Income Tax Assessment Act 1936* (Cth) the *Superannuation Industry (Supervision) Act 1993* (Cth) and the *Retirement Savings Accounts Act 1997* (Cth).

TFN are used to facilitate the effective administration of taxation law and certain aspects of superannuation law. Praemium, a TFN recipient, will only record, collect, use, or disclose TFN information where this is permitted under taxation or superannuation law. An individual's TFN cannot be used to assist with identification of individuals for any other purpose.

Only Praemium employees who need to handle TFN information will be given access to this information.

5. Client access to personal information

Individuals who have provided personal information to Praemium are entitled to access that information or request their information be updated. All client information requests, such as access and correction, must be processed accordingly, including verification of your identity.

Praemium reserves the right to charge for the provision of this information at a reasonable rate based on the nature of the request and how long it will take to fulfill. The charge will be agreed with the requestor and payment will be required before we process the request. We will aim to provide the requested information within 30 days of validation of your request and payment having been received.

There are some circumstances where we may refuse to provide access to information, including cases where legal proceedings are taking place, or providing access may be unlawful, or if providing access would breach another person's privacy. Where we refuse to provide access to information, we will provide a written explanation of our decision.

6. Data breaches

If an unforeseen event occurs which results in the loss, unauthorised access, or disclosure of your personal information, Praemium has processes and mechanisms in place to contain any breach and determine its impact. Where the breach is likely to result in serious harm to you, we will investigate the matter and notify you and the Office of the Australian Information Commissioner pursuant to our obligations under the Privacy Act.

7. Complaints handling process

If you have been affected by a privacy breach by Praemium you can raise a complaint with us by calling Praemium on 1800 571 881, or by writing to the Complaints Handling Officer at:

Email: au.complaints@praemium.com
Post: Praemium, PO Box 322 Collins Street, West Melbourne, 8007

All privacy complaints will be brought to the immediate attention of the Complaints Handling Officer, as well as the Privacy Officer. A privacy complaint will be handled in accordance with Praemium's Complaints Handling Policy, and an appropriate response determined to resolve the issue with you.

If an issue has not been resolved to your satisfaction, you can lodge a complaint with the Australian Financial Complaints Authority (AFCA). AFCA provides fair and independent financial services complaint resolution that is free to consumers.

Website: www.afca.org.au
Telephone: 1800 931 678 (free call)
Email: info@afca.org.au
In writing to: Australian Financial Complaints Authority, GPO Box 3, Melbourne VIC 3001

If you are not satisfied with Praemium's response, you may also be able to lodge a privacy complaint with the Office of the Australian Information Commissioner:

Website: www.oaic.gov.au
Telephone: 1300 363 992
Facsimile: +61 2 6123 5145
Email: enquiries@oaic.gov.au
In writing to: Office of the Australian Information Commissioner, GPO Box 5288, Sydney NSW 2001