PPI Funds Management

Privacy Policy

15 April 2025

Table of Contents

1 Legislation

The *Privacy Act 1988* (**Privacy Act**) requires entities bound by the Australian Privacy Principles to have a privacy Policy. The Office of the Information Commissioner (**OAIC**) is responsible for privacy functions that are conferred by the Privacy Act 1988.

2 What kinds of Personal information is collected and held?

PPI Capital Ltd (**PPI Capital**) may be required to collect and hold personal information in order to provide services to our clients. Generally the kinds of personal information we may collect includes:

- your name, home address, work address, email address, telephone number and signature.

When recruiting employees or appointing contractors PPI Capital may collect and hold personal information such as: the individual's name, contact details, date of birth, citizenship, employment references, civil credit and criminal records, regulatory accreditation (such as RG 146 accreditation for advisers) and driver's licence information, education and employment history. Once appointed we will also collect and hold TFNs, financial information relating to the appointing and banking details for payments.

3 How is it collected?

For our clients, personal information is mainly collected via meetings, telephone, email or correspondence and online forms.

4 Why we collect, hold, use and disclose clients' personal information?

PPI Capital collects, holds, uses and discloses clients' personal information for the purposes of:

- providing financial products or services; and
- complying with our regulatory or legal requirements, including:
    - the *Anti-Money Laundering & Counter-Terrorism Act 2006*
    - the *Corporations Act 2001*
    - the *Australian Securities and Investments Commission Act 2001*
    - the *Bankruptcy Act 1966*
    - the *Tax Laws Amendment (Implementation of the FATCA Agreement) Act 2014*
    - the *Tax Laws Amendment (Implementation of the Common Reporting Standard) Act 2016; and*
    - applicable taxation law.

5 How is it held?

We respect the personal information you have entrusted to us and we have a responsibility to manage and protect that information.

Your personal information will be stored in a secure environment in hard copy, electronically or both. With the exceptions detailed within this policy, your information will only be available to employees of PPI Capital or our service providers on a need-to-know basis in order to perform their obligations and duties.

6 What happens if personal information security is breached?

We implement corrective plans if our security measures are breached or your personal information is lost or inadvertently accessed by an unauthorised person. You and the Privacy Commissioner will be advised if we assess the data breach is likely to cause you serious harm.

Under the first tranche of privacy reforms set out in the *Privacy and Other Legislation Amendment Bill 2024* (Cth) and the *Privacy Act 1988* (Cth) there is a number of new changes that have come into play:

1. A new cause of action which empowers an individual to sue another person where the person has invaded the individual's privacy by intruding upon their seclusion or misusing information relating to them. The new law requires a person to prove the following:
2. There has to be an invasion of privacy either intrusion upon the person's seclusion(eg physical intrusion on their private space) or the misuse of information;
3. The person has a reasonable expectation of privacy in all of the circumstances;
4. The invasion of privacy must be intentional or reckless, rather than merely negligent;
5. The invasion of privacy was deemed serious; and
6. the public interest in the person's privacy outweighs any countervailing public interest (such as freedom of speech or freedom of the media).

The affected person must be an individual or "natural persons". A company cannot be liable under this rule. Any individual or organisation can be sued under this change.

1. Doxxing is now a criminal offence:
2. Doxxing is the use of a carriage service to make available, publish or distribute personal data, where the person engages in the conduct in a way that reasonable persons would regard as being menacing or harassing. This offence will be punishable by up to 6 years' imprisonment.

The Bill also creates a separate doxxing offence where one or more members of a group are targeted due to a belief that the group is distinguished by their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin. This offence is punishable by up to 7 years' imprisonment.

1. Addition of APP 11.3 which provides that 'reasonable steps' in APP 11.1 includes 'technical and organisational measures'.

7 How do you access your personal information and seek correction of it?

Should you wish to know what personal information PPI Capital holds on you, you may request to view this information by contacting our Privacy Officer:

Name:	PPI Privacy Officer
Address:	Level 2, 50 Hindmarsh Square, Adelaide, SA 5000
Tel no.:	(08) 8412 4222
Email:	admin@ppifundsmanagement.com.au

The Privacy Officer will promptly investigate your privacy enquiry and provide you with appropriate answers where required. Should you discover that any information is outdated, incorrect or incomplete you may request to have the personal information corrected and PPI Capital will promptly update our records. You may also contact the Privacy Officer if you have any questions on our compliance with the *Privacy Act 1988 (Cth).*

8 How can I complain about a breach of my privacy?

If you wish to make a complaint about our handling of your personal information you should contact the PPI Capital Privacy Officer as referred to above. If we cannot resolve your complaint then you may raise your issue with the Office of the Australian Information Commissioner.

All privacy breaches that have resulted in or are likely to result in serious harm to any individual affected are '*eligible data breaches*' which must be reported by PPI Capital to the Office of the Australian Information Commissioner.

9 To whom might it be disclosed?

Generally PPI Capital will only disclose your personal information for the purposes of providing our financial products or services to you. This may include disclosing your personal information to related entities of PPI Capital and third parties where necessary to provide you with our financial products or services. These third parties may include government departments and regulatory authorities They may also include our auditors, insurers, custodians, IT providers and third party administrators (service providers).

We may disclose personal information to overseas recipients in order to provide our financial products and/or services. Before disclosing any personal information to an overseas recipient PPI Capital will take reasonable steps to ensure the overseas recipient complies with the Australian Privacy Principles (AAPs) or is bound by a substantially similar privacy regime or you otherwise consent to the overseas disclosure or the disclosure is required or authorised by law.

10 Is sensitive personal information collected?

PPI Capital will not collect sensitive personal information on clients. Sensitive personal information is information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information, biometric information or biometric templates.

11 Notifiable Data Breaches

PPI Capital is required to notify individuals and the Office of the Australian Information Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- there is unauthorised access to or disclosure of personal information held by us (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- this is likely to result in serious harm to any of the individuals to whom the information relates.
- we have been unable to prevent the likely risk of serious harm with remedial action.

We will conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

12 Automated decision-making systems

Automated decision-making systems means a computer program that makes a decision in relation to personal information that could reasonably be expected to significant affect the rights or interests of an individual. If the organisation has an automated decision-making system, then the organisation will need to include information about the kinds of personal information used in the operation of such a computer program, and the kinds of decisions that are made. This is required if there is a computer program which is making, or doing a thing substantially or directly related to the making of, the decision. This means that, if the decision is substantially made or influenced by AI or another automated decision-making system (even if there is a 'human in the loop').

Enforcement mechanisms available to OAIC has been enhanced so as infringement notices for civil penalties for example having a non-compliant privacy policy or failure to issue compliant data breach notice may instigate a civil penalty.

These penalties are expanded to the Federal Court of Australia (FCA) and Family Court of Australia (FCFCOA) powers. The amendments will set out the matters which must be specified in an emergency declaration, including:

- the kinds of personal information that may be handled;
- the entities which may handle the personal information; and
- permitted purposes of the collection, use or disclosure.

13 Privacy Act's Emergency declaration provisions

Privacy Act's emergency declaration provisions has been expanded for the broad sharing of personal information in a declared emergency or disaster.

14 Training

Al staff should be provided regular training on the importance of compliance with the Privacy Act and it's internal policies, particularly given the OAIC's increasingly enforcement-led approach.

15 Civil penalties and enforcement powers

The Bill introduces new lower threshold civil penalties that will align with the severity of the interference with privacy. In determining whether there is an interference severity, factors will be taken into account including the sensitivity of the information and the consequence of the interference with the privacy of the individual.

16 Additional information

Further information on privacy in Australia may be obtained by visiting the website of the Office of the Australian Information Commissioner (**OAIC**) at: http://www.oaic.gov.au/. We regularly review the OAIC website to keep informed of issues and developments in privacy law and changing legal obligations.

--- End of Policy --