The Wealth Designers.

Privacy Policy

TWD Licensee Services Pty Ltd

ABN 88 605 064 480 | AFSL 475964

Effective date	1 November 2026
Policy owner	Privacy Officer

This policy explains how TWD Licensee Services Pty Ltd (TWD, we, us or our), including its representatives, manages personal information under the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). It applies to interactions with us, our authorised representatives, our websites and our staff.

1. Our privacy commitment

We are committed to managing personal information openly, transparently and securely. We maintain practices, procedures and systems designed to support compliance with the APPs and to respond to privacy enquiries and complaints. This policy is available free of charge on our website and, on request, in an alternative form where reasonably practicable.

2. Personal information we collect and hold

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. Depending on our relationship with you, we may collect and hold:

- name, contact details, date of birth, home address and identity verification information;
- tax file number and other government-related identifiers where collection, use or disclosure is authorised by law;
- family circumstances, dependants, estate-planning information and social security entitlements;
- employment, occupation and education information;
- financial needs and objectives, assets, liabilities, income, expenses, insurance, superannuation, investments and transaction information;
- payment and banking information;
- information relating to applications for employment or appointment as an authorised representative, including work history, qualifications, references and background-check information;
- records of communications, complaints and interactions with us;
- website and device information, such as IP address, browser information, cookies, analytics data and online activity; and
- any other information reasonably necessary for our functions or activities, or required or authorised by law.

Sensitive information

Sensitive information may include health information, racial or ethnic origin, genetic information and other information defined as sensitive under the Privacy Act. We will collect sensitive information only where it is reasonably necessary for our functions or activities and you consent, or where another legal exception applies. For example, health information may be required when we assist with an insurance application.

3. How we collect personal information

We generally collect personal information directly from you, including through face to face or online meetings, telephone calls, emails, forms, applications, our websites and digital services. We may also collect information from third parties where you have authorised us, where it is unreasonable or impracticable to collect it directly, or where collection is required or authorised by law. These third parties may include your authorised representatives, product providers, insurers, employers, accountants, solicitors, financial institutions, government agencies, publicly available sources and service providers.

At or before collection, or as soon as practicable afterwards, we will take reasonable steps to notify you of relevant matters required by APP 5, including who we are, the purpose of collection, usual disclosures, any law requiring collection, the main consequences if information is not provided, and how to access this policy.

If you provide us with personal information about another person, you should have authority to do so and, where appropriate, make that person aware of this policy.

Unsolicited personal information

If we receive personal information that we did not solicit, we will determine whether we could have collected it under APP 3. If not, and it is lawful and reasonable to do so, we will destroy or de-identify it as soon as practicable. If we may retain it, we will handle it in accordance with the APPs.

4. Anonymity and pseudonymity

Where lawful and practicable, you may interact with us anonymously or using a pseudonym. This may be possible for general enquiries. It will generally not be practicable where we must verify your identity, provide personal financial advice, process a transaction or comply with legal obligations.

5. Why we collect, use and disclose information

We collect, use and disclose personal information for the primary purpose for which it was collected and for related purposes you would reasonably expect, where you consent, or where required or authorised by law. These purposes may include:

- providing financial advice, financial services and related administration;
- assessing applications, identity and eligibility, and meeting legal and regulatory obligations, including anti-money laundering and counter-terrorism financing requirements;
- communicating with you, managing our relationship and responding to enquiries or complaints;
- processing payments and transactions;
- assessing employment or authorised representative applications;

- quality assurance, audit, risk management, fraud prevention, cybersecurity and business continuity;
- improving our services, websites, technology and client experience; and
- marketing in accordance with APP 7, the Spam Act 2003 and other applicable laws.

6. Who we may disclose information to

We may disclose personal information to recipients including:

- our representatives, employees and related entities where access is required for their functions;
- product issuers, insurers, platforms and financial institutions;
- your authorised advisers and service providers, such as accountants, solicitors, mortgage brokers, stockbrokers and banks;
- professional advisers, auditors, paraplanners, contractors, technology, cloud, data-storage, communications and other service providers;
- government, law enforcement, courts, tribunals, regulators and dispute-resolution bodies where required or authorised by law;
- prospective purchasers or counterparties in a proposed sale, merger or reorganisation, subject to appropriate confidentiality controls; and
- other parties with your consent or at your direction.

Where related entities use shared systems, access is limited to what is required for authorised business purposes and is subject to privacy and information-security controls.

7. Direct marketing

Where permitted by law, we may use or disclose personal information to communicate information about products or services that may interest you, including through email, telephone, SMS, instant messaging, mail, social media and online advertising. We may use service providers to conduct marketing on our behalf.

You may opt out at any time using the unsubscribe facility in a communication or by contacting us. We will not charge you for opting out and will action the request within a reasonable period. You may also ask us to identify the source of personal information used for direct marketing, and we will respond within a reasonable period unless it is impracticable or unreasonable to do so.

8. Government-related identifiers

We will not adopt a government-related identifier, such as a tax file number, Medicare number or pension card number, as our own identifier. We will use or disclose such identifiers only where required or authorised by law or another APP 9 exception applies.

9. Overseas disclosures

We may disclose personal information to service providers or personnel located outside Australia, including in the Philippines and India, and to cloud or technology providers whose processing locations may vary. Before disclosing personal information overseas, we will take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information, unless an exception under APP 8 applies.

Because cloud and networked services may involve multiple or changing processing locations, it may not always be practicable to identify every country in advance. You may contact our Privacy Officer for current information about likely overseas locations relevant to your information.

10. Data quality and correction

We take reasonable steps to ensure personal information is accurate, up to date, complete and, for a use or disclosure, relevant. You may ask us to correct information. We will respond within a reasonable period and will not charge for making a request or correcting information. If we refuse, we will generally give written reasons and explain available complaint mechanisms. You may ask us to associate a statement with the information if we do not make the requested correction, and to notify relevant third parties of a correction where required by APP 13.

11. Security and retention

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Measures may include access controls, authentication, encryption where appropriate, secure premises and systems, confidentiality obligations, staff training, monitoring, backup and incident-response arrangements.

We retain personal information for as long as reasonably required for our functions and legal obligations. Retention periods vary according to the type of information and applicable financial services, taxation, corporate, employment and other requirements. When we no longer need personal information for a permitted purpose, we will take reasonable steps to destroy or de-identify it, unless retention is required by law or the information is contained in a Commonwealth record.

12. Websites, cookies and other technologies

Our websites may use cookies, analytics, pixels, tags, scripts and similar technologies to operate the site, remember preferences, understand usage, improve services and support advertising. These technologies may collect device, browser, IP address, date and time, pages viewed, links selected and similar online activity. Where this information is personal information, we handle it under this policy. You can adjust browser settings to block or delete cookies, although parts of the website may not function as intended.

Our websites may link to external sites. We are not responsible for the privacy practices of third-party sites, and you should review their privacy information.

13. Access to personal information

You may request access to personal information we hold about you. We will respond within a reasonable period and provide access in the manner requested where reasonable and practicable, unless an exception under APP 12 applies. We may require identity verification. If access is refused, we will generally provide written reasons and explain complaint mechanisms. We will not charge for making a request, but may charge a reasonable amount for giving access after notifying you of the likely charge.

14. Data breaches

We maintain procedures to respond to suspected or actual data breaches. If we suspect an eligible data breach, we will carry out a reasonable and expeditious assessment and take appropriate steps to contain and remediate the incident. Where the Notifiable Data Breaches scheme requires notification, we will notify the Office of the Australian Information Commissioner (OAIC) and affected or at-risk individuals as soon as practicable, and provide the information and recommendations required by law.

15. Privacy complaints

Please contact our Privacy Officer if you have a privacy concern or complaint. Provide enough information for us to understand the issue and the outcome you seek. We will acknowledge and investigate the complaint, may request further information, and will communicate the outcome within a reasonable period.

If you are not satisfied with our response, you may contact the OAIC. Depending on the nature of the matter and your eligibility, you may also contact the Australian Financial Complaints Authority (AFCA).

OAIC: www.oaic.gov.au | 1300 363 992 | enquiries@oaic.gov.au

AFCA: www.afca.org.au | 1800 931 678 | info@afca.org.au

16. Contacting us

Privacy Officer	info@twd.com.au
Address	Level 4, 40 Kings Park Road, West Perth WA 6005
Postal Address	PO Box 539, West Perth WA 6872
Phone	08 6363 5300 or 1300 893 000
Website	www.twd.com.au

17. Changes to this policy

We may update this policy when our information-handling practices or legal obligations change. We encourage you to review it periodically on our website.

18. Automated decision-making

From 10 December 2026, additional APP 1 transparency requirements apply where an entity has arranged for a computer program to use personal information to make a decision that could reasonably be expected to significantly affect an individual's rights or interests. TWD will review its arrangements before that date and, if the requirements apply, update this policy to describe the kinds of personal information used and the kinds of decisions made by, or substantially and directly with the assistance of, those programs.