



Privacy Policy

AUSTRALIAN PRIVACY PRINCIPLES

Sidra Wealth Pty Ltd
ABN 11 693 910 600

Version — March 2026

Confidential

Privacy Policy

Sidra Wealth Pty Ltd (ABN 11 693 910 600) Last updated: March 2026

1. Introduction & Scope

Sidra Wealth Pty Ltd (**ABN 11 693 910 600**) ("Sidra Wealth", "we", "us", "our") operates a secure client onboarding portal for the provision of financial advice services.

Financial advice is provided by Mounir Terfas (**Authorised Representative No. 129874**), an authorised representative of PGW Pty Ltd (**AFSL 334512**).

This Privacy Policy explains how we collect, hold, use, and disclose your personal information in accordance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), and our obligations under the *Corporations Act 2001* (Cth) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act).

This policy applies to all personal information collected through our client onboarding portal, by our advisers, and in the course of providing financial advice services.

2. What Personal Information We Collect

We may collect the following categories of personal information:

Identity Information

- Full name, date of birth, gender
- Residential and postal addresses

Contact Information

- Email address, mobile phone number

Government Identifiers

- Tax File Number (TFN)
- Medicare number
- Centrelink Customer Reference Number (CRN)

- Australian Business Number (ABN)

Financial Information

- Employment details, income, and salary
- Assets and liabilities
- Superannuation fund details and balances
- Investment holdings and account details
- Insurance policies (life, TPD, income protection, trauma)
- Centrelink benefits and entitlements

Estate Planning

- Will and power of attorney status
- Beneficiary nominations

Risk Profile

- Responses to risk profile questionnaire
- Assessed risk category (Conservative, Moderately Conservative, Balanced, Growth, High Growth)

Documents

- Uploaded identification documents (PDF, images)

Technical Data

- IP address, browser user agent
- Session timestamps and activity logs

3. How We Collect Personal Information

We collect personal information:

- **Directly from you** — through our secure onboarding portal when you complete your risk profile questionnaire and fact-find form
- **From your financial adviser** — when your adviser creates an engagement and provides initial details on your behalf
- **Automatically** — technical data such as IP address, session timestamps, and browser user agent collected when you access the portal

We will not collect personal information without your knowledge or consent, unless required or authorised by law.

4. Why We Collect Personal Information

We collect your personal information for the following primary purposes:

- To provide you with personalised financial advice
- To prepare a Statement of Advice (SOA) and other advice documents
- To assess your risk profile and investment suitability
- To complete your client onboarding and fact-find
- To verify your identity as required under AML/CTF legislation
- To comply with our obligations under the *Corporations Act 2001* (Cth), including record-keeping and reporting requirements
- To manage and administer your financial products and services
- To communicate with you about your financial advice engagement

We will only use or disclose your personal information for a purpose other than the primary purpose of collection if you would reasonably expect us to use or disclose the information for a secondary purpose, or if you have consented, or if required or authorised by law.

5. Tax File Number (TFN) — Special Disclosure

We may ask you to provide your Tax File Number. Under the *Taxation Administration Act 1953* (Cth) and the Privacy (Tax File Number) Rule 2015:

- **Provision is voluntary** — you are not required to provide your TFN
- **Consequences of not providing** — if you choose not to provide your TFN, we may not be able to complete certain aspects of your financial plan, and you may have tax withheld at a higher rate on some investment income
- **Restricted use** — your TFN will only be used for lawful purposes related to your financial advice, superannuation, investments, and taxation
- **Security** — your TFN is encrypted at rest using AES-256 encryption and is masked in all display contexts (shown as XXX XXX XX_)
- **No disclosure** — we will not disclose your TFN to any third party except as required by taxation law

6. Government Identifiers (Medicare, CRN)

We may collect your Medicare number and Centrelink Customer Reference Number (CRN) to:

- Assess your eligibility for government benefits relevant to your financial plan
- Coordinate with Centrelink regarding any income or asset impacts of financial advice recommendations

In accordance with APP 9, we will not use government identifiers as our own identifier for you, and will only use or disclose them as required by law or for the purposes for which they were collected.

7. How We Hold & Protect Your Information

We take reasonable steps to protect your personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure. Our security measures include:

- **Data hosting** — your data is stored in a PostgreSQL database hosted by Supabase on Amazon Web Services (AWS) in the Sydney (ap-southeast-2) region, keeping your data on Australian soil
- **Encryption in transit** — all data transmitted between your browser and our servers is encrypted using TLS (HTTPS)
- **Encryption at rest** — sensitive fields including TFN, Medicare number, and CRN are encrypted using AES-256 encryption with a dedicated field encryption key
- **Session security** — JWT-based sessions with 30-minute inactivity timeout and 4-hour absolute timeout; magic link authentication (no passwords stored for clients)
- **Access controls** — adviser authentication is protected with bcrypt-hashed passwords and IP-based rate limiting
- **Audit trail** — an append-only audit log records all significant actions, including IP address, user agent, actor, and action details
- **File uploads** — restricted to PDF and image formats with a 10 MB size limit; stored in a private Supabase Storage bucket

8. Who We Share Your Information With

We may share your personal information with:

- **PGW Pty Ltd** (AFSL 334512) — our licensee, as required for compliance and supervision obligations
- **Product providers** — superannuation funds, investment platforms, and insurance providers as necessary to implement your financial advice
- **Government and regulatory bodies** — the Australian Taxation Office (ATO), AUSTRAC, ASIC, or other bodies where required by law
- **Professional advisers** — accountants, lawyers, or other professionals you have authorised us to communicate with

We do not sell, rent, or trade your personal information to third parties for marketing purposes.

9. Overseas Disclosure

While your data is hosted on servers located in Australia (AWS Sydney region), some of the technology services we use are provided by companies based overseas:

- **Supabase Inc.** (United States) — database hosting and file storage. While Supabase is a US-incorporated company, the database servers storing your data are located in Sydney, Australia
- **Resend Inc.** (United States) — transactional email delivery for magic link authentication emails

In accordance with APP 8, before disclosing personal information to an overseas recipient, we take reasonable steps to ensure they do not breach the APPs in relation to that information. We remain accountable for the handling of your personal information by these service providers.

10. Direct Marketing

We do not use your personal information for direct marketing purposes without your consent. If we ever do communicate with you for marketing purposes, you will have the right to opt out at any time by:

- Contacting us using the details in Section 17
- Using any unsubscribe mechanism in the communication

11. Data Retention & Destruction

We retain your personal information in accordance with our legal obligations:

DATA CATEGORY	RETENTION PERIOD	LEGAL BASIS
Financial advice records, SOAs, fact-find data	7 years after the advice relationship ends	<i>Corporations Act 2001 s. 947D</i>
AML/CTF identity verification records	7 years after the relationship ends	<i>AML/CTF Act 2006 s. 107</i>
Tax file numbers and tax records	7 years after last use	<i>Taxation Administration Act 1953</i>
Audit logs	7 years	Compliance and dispute resolution
Session and technical logs	12 months	Operational security

When personal information is no longer needed for any purpose for which it may be used or disclosed under the APPs, and we are not required by law to retain it, we will take reasonable steps to destroy or de-identify the information.

12. Your Rights

Under the APPs, you have the right to:

- **Access your personal information** (APP 12) — you may request access to the personal information we hold about you
- **Correct your personal information** (APP 13) — you may request that we correct any inaccurate, out-of-date, incomplete, irrelevant, or misleading personal information

- **Opt out of direct marketing** (APP 7) — you may request that we stop using your personal information for direct marketing
- **Make a privacy complaint** (APP 1.4(e)) — you may complain if you believe we have breached the APPs

13. How to Access or Correct Your Information

To request access to or correction of your personal information:

1. Contact us using the details in Section 17
2. We will acknowledge your request within 7 days
3. We will respond to your request within 30 days
4. We will provide access in the manner you have requested, where reasonable and practicable
5. If we refuse access or correction, we will provide written reasons

There is no fee for making a request. However, we may charge a reasonable fee for providing access if your request requires substantial effort (we will advise you of any fee in advance).

14. How to Make a Privacy Complaint

If you believe we have breached the APPs or mishandled your personal information:

1. **Contact us first** — lodge a complaint using the details in Section 17. We will acknowledge your complaint within 7 days and investigate and respond within 30 days
2. **Office of the Australian Information Commissioner (OAIC)** — if you are not satisfied with our response, you may lodge a complaint with the OAIC at www.oaic.gov.au or by calling 1300 363 992
3. **Australian Financial Complaints Authority (AFCA)** — for complaints relating to financial services, you may also contact AFCA at www.afca.org.au or by calling 1800 931 678

15. Notifiable Data Breaches

In accordance with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988*, if we become aware of a data breach that is likely to result in serious harm to any individual whose personal information is involved, we will:

- Take immediate steps to contain the breach and mitigate harm
- Assess the breach to determine if notification is required
- Notify the OAIC and affected individuals as soon as practicable if the breach is assessed as an eligible data breach

16. Updates to This Policy

We may update this policy from time to time to reflect changes in our practices, legal requirements, or technology. When we make material changes:

- The updated policy will be published on our portal at [/privacy](#)
- The "Last updated" date at the top of this policy will be revised
- Where practicable, we will notify you of significant changes

We encourage you to review this policy periodically.

17. Contact Us

For any privacy-related queries, requests, or complaints, please contact our Privacy Officer:

Privacy Officer Sidra Wealth Pty Ltd ABN 11 693 910 600

Email: privacy@sidrawealth.com.au **General enquiries:** portal@sidrawealth.com.au **Website:**
www.sidrawealth.com.au