PRIORITY1 WEALTH MANAGEMENT GROUP

Privacy Policy

Australian financial services privacy framework

Document owner	Privacy Officer
Version	1.0 draft
Effective date	10 December 2026 (proposed, subject to approval)
Next review	10 December 2027 (proposed)
Approved by	Corin Jacka

DRAFT FOR INTERNAL AND LEGAL REVIEW ONLY | 25 November 2026 | Not approved for publication.

1. Introduction and scope

Priority1 Wealth Management Group (Australia) Pty Ltd (ABN 26 130 448 314; AFSL 324472) is the Australian financial services licensee referred to in this policy as Priority1. Priority1 Wealth Management Group Pty Ltd (ABN 55 006 469 978) is a corporate authorised representative (CAR) which has adopted this policy. This policy applies to both the licensee and the corporate authorised representative, including their staff and representatives acting on their behalf. We are committed to protecting personal information under the Privacy Act 1988 (Cth), the Australian Privacy Principles and the Notifiable Data Breaches scheme.

This policy explains the kinds of personal information we collect and hold, how and why we collect, use and disclose it, how we protect it, and how individuals may access or correct their information or make a privacy complaint.

This policy applies to personal information about clients, prospective clients, beneficiaries, family members, representatives, advisers, employees, contractors, suppliers and other individuals with whom we deal. Additional collection notices may apply to a particular product, service, website, application or activity. If there is an inconsistency, the more specific notice applies to that activity to the extent of the inconsistency.

2. Key definitions

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information is true and whether or not it is recorded in a material form.

Sensitive information includes health and genetic information, biometric information used for identification, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or practices, criminal record, and membership of political, professional or trade associations or trade unions.

Government-related identifiers include identifiers such as a tax file number, Medicare number, passport number and driver licence number.

3. Personal information we collect and hold

The information we collect depends on our relationship with you and the products or services involved. It may include:

- identity details, including name, date of birth, residential address, citizenship and residency status, photographs and identity documents;
- contact details and communication preferences;
- family, dependent, beneficiary, estate planning and relationship information;
- employment, occupation, education and professional information;
- financial information, including income, expenses, assets, liabilities, bank details, superannuation, investments, taxation information, transaction history and financial objectives;
- advice information, including goals, needs, priorities, risk profile, preferences and records of advice and instructions;
- information about borrowing and liabilities where relevant to financial planning (we do not provide credit assistance);
- health, medical, lifestyle, insurance and claims information, where relevant to insurance advice, applications or claims;
- government-related identifiers where required or authorised by law;
- records of meetings, calls, correspondence, complaints, consents and interactions with us;
- online and technical information, such as IP address, device and browser information, login activity, cookies, pages visited and form submissions; and
- information about advisers, representatives, employees, contractors, suppliers and job applicants.

Sensitive information

We only collect sensitive information when it is reasonably necessary for our functions or activities and you consent, or where collection is otherwise permitted or required by law. For example, health and lifestyle information may be required for life insurance advice, underwriting or claims.

Information about other people

If you provide personal information about another person, such as a spouse, dependent or beneficiary, you should be authorised to do so and should make that person aware of this policy and any relevant collection notice, unless it is unreasonable or impracticable to do so.

4. How we collect personal information

We generally collect personal information directly from you, including when you:

- meet or speak with us;
- complete fact finds, application forms, identity checks or other documents;
- use our website, online forms, portals, applications or interactive tools;
- send us emails, messages, documents or instructions;
- apply for, acquire, use or review a product or service; or
- make an enquiry, complaint, access request or correction request.

We may also collect information from third parties where you consent, where you would reasonably expect us to do so, or where the law permits. These parties may include your authorised representatives, accountant, solicitor, employer, product providers, insurers, superannuation funds, lenders, health professionals, identity verification providers, referrers, public registers, social media, regulators and service providers.

Unsolicited information

If we receive personal information that we did not request, we assess whether we could have collected it under the APPs. If not, and it is lawful and reasonable to do so, we destroy or de-identify it.

Anonymity and pseudonyms

You may deal with us anonymously or using a pseudonym where lawful and practicable, such as for a general enquiry. However, we will not be able to provide some of our services such as personal financial advice or arrange a financial product unless you accurately identify yourself. You need to provide us with full and accurate information.

5. Why we collect, hold, use and disclose information

We collect, hold, use and disclose personal information where reasonably necessary to:

- provide financial advice and related services, including preparing, implementing and reviewing advice;
- assess needs, objectives, financial circumstances and eligibility and suitability for products or services;
- arrange, administer and manage investments, superannuation, insurance and other financial products;
- verify identity and comply with taxation, anti-money laundering and counter-terrorism financing, sanctions, record-keeping and other legal obligations;
- communicate with you and manage our relationship, accounts, fees, payments and service arrangements;
- handle enquiries, complaints, disputes, claims, incidents and legal proceedings;
- prevent, detect and investigate fraud, cyber incidents, unlawful activity and misconduct;
- conduct compliance reviews, audits, quality assurance, training, research, data analysis and business planning;
- manage advisers, representatives, employees, contractors and suppliers;
- protect our lawful interests and facilitate a proposed or completed sale, transfer or restructure of a business, subject to confidentiality and legal requirements; and

- carry out other purposes notified to you or to which you consent.

If you do not provide information

You are not required to provide all information we request. However, if information is incomplete, inaccurate or not provided, we may be unable to verify your identity, provide or implement appropriate advice, arrange a product or service, or continue our relationship with you.

6. Use and disclosure

We generally use or disclose personal information for the primary purpose for which it was collected, for a related secondary purpose - or, for sensitive information, a directly related secondary purpose - that you would reasonably expect, with your consent, or where required or authorised by law.

Depending on the circumstances, recipients may include:

- authorised representatives, corporate authorised representatives and related entities;
- financial product issuers, platform operators, superannuation trustees, fund managers, insurers, reinsurers, lenders, banks, stockbrokers, custodians and payment providers;
- paraplanners, administration providers, identity verification services, cloud, software, cybersecurity, data storage, printing, mailing and archiving providers;
- professional advisers and service providers, including accountants, solicitors, auditors, compliance consultants, actuaries, medical practitioners and debt recovery providers;
- persons acting for you, including an attorney, guardian, executor, trustee, accountant or solicitor;
- regulators, government agencies, law enforcement bodies, courts, tribunals and external dispute resolution bodies, where required or authorised; and
- prospective purchasers, successors or counterparties in a business sale, transfer or restructure, subject to appropriate confidentiality controls.

We do not sell personal information for unrelated third-party marketing.

7. Direct marketing

We may use personal information, other than sensitive information unless you consent, to tell you about products, services, events, insights or opportunities that we reasonably believe may interest you, where permitted by law. Communications may be delivered by email, post, telephone, SMS or other electronic means.

You can opt out at any time by using the unsubscribe facility in a communication or contacting us. We will action the request within a reasonable period and will not charge you. You may also ask us, where applicable, to identify the source of personal information used for direct marketing.

8. Government-related identifiers

We only collect, use or disclose government-related identifiers where required or authorised by law or where otherwise permitted under the APPs. We do not adopt a government-related identifier as our own identifier of an individual.

9. Overseas disclosure and access

We may disclose personal information to, or allow it to be accessed or stored by, service providers located outside Australia, including for paraplanning, administration, software, cloud hosting, cybersecurity, provision of AI tools and services, technical support and data processing.

The Philippines, including Cebu, is a country in which offshore administrative staff may access personal information. [VERIFY OTHER LIKELY COUNTRIES OF DISCLOSURE OR ACCESS THROUGH CLOUD, AI, SOFTWARE SUPPORT AND SUBPROCESSORS.]

Before disclosing personal information overseas, we will take reasonable steps required by law to ensure the recipient handles the information consistently with the APPs, unless an exception applies. Overseas recipients may be subject to different privacy laws, and foreign governments or courts may be able to access information under local law.

Our offshore administration provider is VA Platinum Pty Ltd. Its personnel working from the Cebu office in the Philippines can access relevant client information in Worksorted, AstuteWheel, SharePoint and Marloo, including financial, identity, insurance and health information where necessary for their assigned duties. VA Platinum maintains privacy and data breach procedures and contractual confidentiality obligations. Its data protection breach management policy is available at https://www.vaplatinum.com.au/data-protection. [VERIFY ANY OTHER OVERSEAS ACCESS THROUGH OTHER SERVICE PROVIDERS OR SUBPROCESSORS.]

10. Website, cookies and analytics

Our websites and applications may use cookies and collect information submitted through online forms, pixels, web beacons, log files and similar technologies. These technologies can collect IP address, device and browser details, referring pages, pages viewed, dates and times, approximate location, interactions and preferences.

We use this information to operate and secure our online services, understand use, diagnose issues, improve content and functionality, measure campaigns and provide relevant communications. You can control cookies through your browser or device settings, although disabling cookies may affect functionality.

Priority1 does not currently use Google Analytics or advertising pixels, according to its internal operational review. Basic technical logs or cookies necessary to operate its website or third-party services may still be used.

Links to third-party websites are provided for convenience. We are not responsible for the privacy practices of third parties and encourage you to review their privacy policies.

11. Automated decisions and artificial intelligence

Commented [DH1]: We note that the 'automated decision' disclosures don't need to be disclosed until the relevant amendments take place on 10 December 2026.

We use Worksorted for client and workflow records; AstuteWheel for client information and financial modelling; Delta Portfolios for investment research and forecasts; Microsoft 365/SharePoint and the licensed business version of Copilot for document and information work; and Marloo for generating draft meeting and advice documents. These systems may process client identity, contact, financial, superannuation, investment, risk-preference, insurance and meeting information as relevant. Marloo produces draft documents for adviser review. The adviser reviews and approves all financial strategies, recommendations and advice before release. We do not use automated client risk-profiling, product-selection or eligibility decisions as a standalone decision process.

From 10 December 2026, where we arrange for a computer program to use personal information to make a decision, or do something substantially and directly related to making a decision, that could reasonably be expected to significantly affect an individual's rights or interests, we disclose the required categories below. This can apply even where an adviser reviews the software output. The descriptions must be confirmed against our actual processes before publication.

We apply access, confidentiality and security controls to approved software and AI tools. We use a business-licensed Microsoft Copilot environment rather than consumer AI accounts for identifiable client information. Priority1 understands its AI providers do not use client information to train their models.

Kinds of decisions made solely by computer programs: Priority1 does not knowingly use computer programs to make significant financial advice, eligibility or client-acceptance decisions without adviser review and approval.

Kinds of decisions for which computer programs may do something substantially and directly related to decision-making: financial strategy and retirement projections, investment and portfolio modelling, product comparisons, and the preparation of draft advice recommendations. Such outputs can materially inform the advice and recommendations approved by the adviser. The kinds of personal information used may include age, family circumstances, income, expenditure, assets, liabilities, tax, superannuation, investment objectives, risk preferences and, where relevant, insurance and health information. This disclosure applies where such

decisions could reasonably be expected to significantly affect an individual's rights or interests, even when the output is reviewed by an adviser.

12. Security, retention and destruction

We hold personal information electronically in client-management systems, document-management systems and other secure storage services, including those operated by service providers, and in physical files stored securely at our offices or secure off-site storage facilities. We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure. Measures may include:

- role-based access controls and least-privilege access;
- multi-factor authentication, strong passwords and secure client portals;
- encryption and secure transmission where appropriate;
- firewalls, malware protection, monitoring, patching and backups;
- physical access controls and secure storage of paper records;
- staff and representative training, confidentiality obligations and incident reporting;
- supplier due diligence and contractual privacy and security requirements; and
- cyber incident and data breach response procedures.

We retain personal information as needed for our services and applicable legal, regulatory, dispute and professional obligations. Some financial advice and identification records have minimum retention requirements, commonly at least seven years in relevant circumstances. Priority1 has documented retention and data breach procedures. When information is no longer required, we take reasonable steps to securely destroy or de-identify it, unless law requires or authorises retention. [

13. Data breaches

We maintain procedures to identify, contain, assess and respond to suspected data breaches. Where we have reasonable grounds to believe an eligible data breach has occurred, we will notify affected or at-risk individuals and the Office of the Australian Information Commissioner as required by the Notifiable Data Breaches scheme. A notification will include recommended steps individuals can take in response, where practicable.

14. Accessing and correcting personal information

You may request access to the personal information we hold about you and ask us to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. We may ask you to verify your identity and clarify the information requested.

We do not charge for making an access request or correcting information. Reasonable costs of giving access may be charged after advance notice. We aim to respond within 14 days where practicable and otherwise within a reasonable period, generally within 30 days. [CONFIRM WHETHER THE 14-DAY TARGET REMAINS THE OPERATING SERVICE STANDARD.]

In limited circumstances permitted by law, we may refuse access or correction. If we refuse access, refuse access in the manner requested, or refuse a correction request, we will provide written notice explaining the available complaint mechanisms and our reasons, except to the extent that giving reasons would be unreasonable in the circumstances.. If we refuse a correction request, you may ask us to associate a statement with the information noting that you consider it inaccurate, out of date, incomplete, irrelevant or misleading.

15. Privacy enquiries and complaints

If you have a question, want to exercise a privacy right or believe we have breached the APPs or this policy, contact our Privacy Officer using the details below. Please provide enough information to identify the issue and the outcome you seek.

We will acknowledge a complaint promptly, investigate it fairly and aim to provide a substantive written response within 30 days. If more time is reasonably required, we will tell you why and provide an updated timeframe.

If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC):

- Website: www.oaic.gov.au
- Phone: 1300 363 992
- Post: GPO Box 5288, Sydney NSW 2001

For a complaint connected with financial services, you may also be able to contact the Australian Financial Complaints Authority (AFCA):

- Website: www.afca.org.au
- Phone: 1800 931 678
- Post: GPO Box 3, Melbourne VIC 3001

16. Contact details

Privacy Officer	Corin Jacka
Organisation	Priority1 Wealth Management Group (Australia) Pty Ltd
ABN	26 130 448 314
AFSL / ACL	AFSL 324472; no credit assistance provided
Email	info@priority1.net.au
Phone	03 9725 9078
Post	PO Box 375, Croydon VIC 3136

17. Changes to this policy

We may update this policy to reflect changes in law, technology, our operations or information-handling practices. The current version will be available free of charge on our website and, on request, in an alternative form where reasonable.

Website: www.priority1.net.au. The current privacy policy will be made available on the website. [CONFIRM PUBLIC POLICY PAGE LOCATION WHEN UPLOADED.]

-