DB Advisers

Our knowledge for your benefit

Privacy Policy

Table of Contents

1 About this policy

At **DB5 Advisers Pty Ltd** (**Licensee**), protecting your personal information is fundamental to how we operate. This Privacy Policy explains our commitment to safeguarding your privacy under Australian law, specifically the Privacy Act 1988 and the Australian Privacy Principles.

We recognise that trust is the cornerstone of our client relationships. This policy outlines our approach to collecting, managing, using and protecting your personal information throughout our professional relationship. We also detail your privacy rights and how you can exercise them.

Our business centres on helping clients navigate complex financial decisions and build wealth for their future. To deliver tailored advice that genuinely serves your interests, we need to understand your unique financial circumstances, goals and personal situation. This necessitates collecting and using various types of personal information about you.

Beyond our primary advisory services, we may also process your information for operational purposes including:

- client service delivery and support;
- business administration and record keeping;
- regulatory compliance and reporting;
- staff training and quality assurance;
- complaint resolution and dispute management.

This policy is subject to regular review to ensure it remains current with legislative changes and evolving business practices. Updates will be made as needed.

2 What information do we handle

We work with different types of client data to provide professional services. Under Australian legislation, personal information encompasses details and opinions relating to people who can be identified or are capable of being identified, irrespective of accuracy or documentation format.

The personal information we typically collect and manage may include:

Information Category	Details
Identity Information	Full name, date of birth, place of birth, and the identification documents we sight or retain to verify your identity
Contact Details	Residential and postal addresses, email addresses, telephone numbers
Government Identifiers	Tax File Number
Financial Information	Income, expenses, assets, liabilities, investment holdings
Employment Details	Occupation, employer information, employment history

Family Information	Marital status, dependants, beneficiaries and estate planning details, which may include personal information about people other than you
Health Information	Medical details provided by you, and health records and assessments obtained for insurance purposes
Advice and Service Records	The advice we provide, the information it was based on, and our file notes, correspondence and records of meetings and calls
Compliance Records	Identity verification records kept under anti-money laundering legislation, complaints records, and other records we keep to meet our obligations as a financial services licensee

We may also collect sensitive information where necessary for specific services, such as health information for insurance advice or recommendations. Such collection only occurs with your express consent and where legally permitted.

Your Tax File Number is a government related identifier. We collect it only where the law requires or authorises it, or where it is needed to establish or administer a product on your behalf. We do not adopt it as our own means of identifying you, and we do not use or disclose it except as permitted by Australian Privacy Principle 9 and the Privacy (Tax File Number) Rule 2015. Where we sight or retain an identification document that carries a government related identifier - a driver's licence or Medicare card, for example, we treat that identifier the same way.

Some of the information we hold is about people other than you, including your spouse or partner, your dependants and the beneficiaries you nominate. Where you give us information about another person, we ask that you tell them we hold it and direct them to this policy. Anyone whose information we hold has the same rights of access and correction set out in section 5, and can contact us using the details in section 7.

3 Information sources and collection

3.1 Where your information comes from

Client data reaches us via several pathways as part of delivering our advisory services. Most commonly, you provide details directly during meetings, through completed forms, or via phone and email correspondence. This direct approach ensures accuracy and allows for immediate clarification of any questions.

External sources may also provide relevant details when authorised or legally required, such as:

- **Financial institutions:** Banks, super funds, investment platforms, insurance companies
- **Professional advisers:** Accountants, solicitors, other financial advisers
- **Government agencies:** Australian Taxation Office, Centrelink, regulatory bodies
- **Family members:** Spouse, adult children or other relatives (with appropriate authority)
- **Employers:** For employment verification and superannuation details

- **Overseas pension schemes:** Scheme administrators, trustees and their advisers, where you have engaged us in relation to an international pension transfer
- **Product providers:** Platform operators, insurers and fund managers holding products in your name

We maintain strict protocols around third-party data collection, ensuring proper authorisation exists before accessing information from external sources. All data gathering activities align with privacy legislation and professional standards.

3.2 Information we collect through our website and digital channels

When you visit our website, complete an online form or open an email from us, we may collect information automatically. This includes your IP address, browser and device type, the pages you view, and the date and time of your visit. We use cookies and similar technologies for this purpose.

We use this information to operate and improve the website, to understand how it is being used, and to keep it secure. Most of it does not identify you personally, but where it is combined with other information we hold about you, we treat it as personal information and handle it in accordance with this policy.

You can set your browser to refuse cookies or to notify you when one is being set, although parts of our website may not work properly if you do. Where we use third-party analytics or email delivery services, those providers may collect this information on our behalf. Section 4 sets out who we disclose information to.

3.3 Unsolicited information handling

Occasionally, we may receive client details without our request or initiation. Upon receipt of such material, we conduct an immediate assessment to determine whether we possess legitimate grounds for retaining this data under privacy legislation.

Where no valid collection basis exists, we implement secure deletion or de-identification procedures promptly, subject to legal constraints and practical considerations.

3.4 Informing you about collection

Transparency is central to our privacy practices. We ensure you understand how and why we collect your information by providing clear notices that explain:

- who we are and our contact details
- what specific details we're requesting and why
- legal requirements driving our data needs
- how this information supports our service delivery
- potential impacts if certain details aren't provided
- third parties who might receive this information
- your options for accessing and updating records
- how to raise concerns about our practices
- any sharing of your information with overseas recipients.

We generally give this notice in our Financial Services Guide, and at the point we collect information from you. Where we collect information about you from someone else, we take reasonable steps to notify you of the matters above unless you would already be aware of them. This ensures you can make informed decisions about sharing information with us.

3.5 Anonymity and pseudonymity

The law gives you the option of dealing with us anonymously, or under a pseudonym, where it is lawful and practicable for us to allow it.

We understand some clients prefer maintaining anonymity, though this creates significant barriers to delivering our core services. Financial advice inherently requires understanding individual circumstances, goals and risk profiles.

Legal obligations also mandate client identification and verification processes under anti-money laundering legislation. These requirements make anonymous service delivery impractical for most advisory relationships.

While we can provide general information and educational materials without identification, personalised advice and implementation services require full client disclosure to ensure compliance and appropriateness.

The same constraints apply to dealing with us under a pseudonym. Where you have concerns about how you are identified in our records or correspondence, raise them with our Privacy Officer and we will accommodate them where we can.

3.6 Consequences of limited information

Providing complete and accurate information enables us to deliver comprehensive, tailored advice that serves your best interests. If you choose not to provide certain information, this may impact our ability to:

- assess your financial needs and circumstances accurately;
- recommend appropriate strategies and products;
- comply with legal obligations regarding client assessment;
- provide ongoing monitoring and review services;
- assist with insurance claims or benefit applications.

We will always explain the implications of not providing specific information so you can make informed decisions about your privacy preferences.

4 Information uses and disclosure

We use and disclose personal information for the purposes set out in this section, for purposes directly related to them, where you have consented, and where we are required or authorised by law.

Primary uses include:

- conducting financial needs analysis and goal setting;
- developing and presenting strategic recommendations;
- implementing agreed strategies and monitoring progress;

- facilitating product applications and account establishment;
- providing ongoing advice and portfolio reviews;
- meeting regulatory reporting and compliance obligations;
- handling complaints and disputes;
- conducting internal audit, compliance monitoring and quality assurance.

4.1 Who we disclose your information to

We disclose personal information only where it is necessary for one of the purposes set out above, where you have consented, or where we are required or authorised by law. The organisations we may disclose your information to include:

Product and service providers: product issuers, platform operators, superannuation and pension trustees, insurers and fund managers, so that we can make applications, effect transactions and administer your holdings;

Overseas pension schemes: scheme administrators, trustees and their advisers, where you have engaged us in relation to an international pension transfer. Section 4.3 explains how we handle information sent overseas;

Your other advisers: your accountant, solicitor, mortgage broker or other adviser, where you have asked us to work with them or have authorised us to do so;

Our service providers: paraplanning, research, administration, information technology, cloud hosting, document storage, email and archiving providers engaged by us, who may access personal information in the course of providing those services;

Regulators, auditors and insurers: the Australian Securities and Investments Commission, the Australian Taxation Office, AUSTRAC, the Office of the Australian Information Commissioner, the Australian Financial Complaints Authority, our external auditors, our professional indemnity insurer and our legal advisers;

Others you authorise: anyone else you have authorised, and anyone to whom we are required or permitted to disclose information by law.

Anyone who receives personal information from us is bound by confidentiality and privacy obligations, whether under their contract with us or under the Privacy Act. We select our service providers with those obligations in mind and hold them to the standards in this policy.

If we sell or transfer our business, or any part of it, personal information may be disclosed to the purchaser or to a prospective purchaser and their advisers as part of that transaction. Where the law requires us to notify you or to obtain your consent before doing so, we will.

4.2 Marketing and promotional activities

We may contact you about products, services, market insights and educational opportunities that align with your interests and financial objectives.

All marketing communications include clear opt-out instructions, and you can withdraw consent for marketing contact at any time by contacting us.

We do not use or disclose sensitive information, including health information, for direct marketing purposes without your consent. We do not sell your personal information, and we do not disclose it to other organisations for their own direct marketing.

You may ask us where we obtained your information, and we will tell you unless it is unreasonable or impracticable to do so. Our electronic marketing complies with the Spam Act 2003, and where we make marketing calls we comply with the Do Not Call Register Act 2006.

4.3 International sharing of information

We specialise in international pension transfers, so we may need to send your information overseas to service providers or other third parties who operate or hold data outside Australia. The countries to which we may send your information are:

- The United Kingdom
- Malta
- Gibraltar
- New Zealand

We will tell you if this list changes, and the current list is always the one set out in this policy.

5 Your rights and responsibilities

5.1 Maintaining information quality

Accurate, current and complete information is essential for effective financial advice. We have established procedures to ensure information quality including regular data validation, client confirmation processes and systematic reviews of stored information.

You can help maintain information accuracy by promptly notifying us of any changes to your circumstances and reviewing information we provide for verification. We will correct any errors identified and can notify third parties of corrections where appropriate.

5.2 Security and protection measures

Protecting your information from unauthorised access, loss or misuse is a critical responsibility. Our security framework incorporates multiple protective measures:

Technical Safeguards:

- Multi-factor authentication and access controls;
- Secure backup and disaster recovery systems;
- Network intrusion detection.

Administrative Safeguards:

- Staff privacy and security training;
- Incident response and breach management procedures;
- Restrictions on access, so that personal information is available only to those who need it;
- Confidentiality obligations in our employment and contractor agreements;

- Due diligence on service providers before we engage them, and privacy and security obligations in our arrangements with them.

Physical Safeguards:

- Secure storage of paper records and identification documents;
- Secure destruction of paper records when they are no longer required;
- Access controls over our premises and equipment, and controls over the removal of devices and records from them.

No method of storage or transmission is completely secure. While we take reasonable steps to protect your personal information, we cannot guarantee absolute security. If you believe your information has been compromised, contact us immediately using the details in section 7.

5.3 Access and correction rights

You have the right to request access to personal information we hold about you and to seek correction of any inaccuracies. We aim to respond to access requests promptly and comprehensively.

To make a request, contact our Privacy Officer using the details in section 7. We may ask you to verify your identity before we release any information. We will acknowledge your request and respond within 30 days. Where a request is complex we will tell you if we need longer, and why.

We do not charge for making a request. We may charge a reasonable fee for the cost of retrieving and supplying the information, for example where a request covers a long period or a large volume of records. We will tell you what the charge will be before we incur it, and you can withdraw or narrow your request at that point.

In limited circumstances we may refuse a request - for example where giving access would have an unreasonable impact on another person's privacy, where the information relates to anticipated legal proceedings, or where the law requires or authorises us to refuse. If we refuse, we will tell you in writing why, and how you can complain about that decision. Where we cannot give access in the form you asked for, we will discuss an alternative with you.

If we correct information we have previously disclosed to another organisation, you can ask us to notify that organisation of the correction, and we will do so unless it is impracticable or unlawful. If we decline to correct information, we will tell you why, and you can ask us to attach a statement to the record noting that you consider it inaccurate.

5.4 How long we keep your information

We keep personal information for as long as we need it for the purposes described in this policy, and for as long as the law requires us to keep it. As a financial services licensee we are generally required to keep client records for at least seven years. Where a record relates to advice we have given you, the retention period generally runs from the date we stop providing services to you.

When we no longer need personal information and are no longer required to keep it, we destroy it or de-identify it securely. Paper records are destroyed securely, and electronic records are deleted from our systems and, in the ordinary course of our backup cycle, from our backups.

5.5 Incident response and breach management

Despite our protective measures, security incidents can occur. A privacy incident involves unauthorised access, loss or misuse of client information. This could include stolen devices, system intrusions or accidental disclosure to wrong recipients. We begin assessing any suspected incident as soon as we become aware of it, and complete that assessment within 30 days at the latest, to determine whether it is an eligible data breach under the Notifiable Data Breaches scheme. Where serious harm is likely despite our remedial actions, we notify affected clients and the Office of the Australian Information Commissioner as required by law.

Our response focuses on containing the incident, preventing further harm and implementing improvements to reduce future risks. Our Data Breach Response Policy sets out how we identify, contain, assess and report incidents, and we record all incidents in our Data Breach Register.

6 Making a privacy complaint

If you believe we have breached the Australian Privacy Principles or otherwise mishandled your personal information, we want to hear about it. You can complain to us in writing, by telephone or in person, using the contact details in section 7. You do not need to put your complaint in writing, although it helps us if you do.

We will acknowledge your complaint promptly, and our Privacy Officer will investigate it. We will give you a written response within 30 days, setting out our findings, the reasons for them, and any action we propose to take. If we need longer than 30 days we will tell you before that period ends, explain why, and give you a new date.

We record privacy complaints in our complaints register and review them to identify whether any change to our practices is warranted. Making a complaint costs you nothing and will not affect the services we provide to you.

If you are not satisfied with our response, or if we have not responded within 30 days, you can take the matter further:

Office of the Australian Information Commissioner:

GPO Box 5288, Sydney NSW 2001

1300 363 992

www.oaic.gov.au

Australian Financial Complaints Authority:

GPO Box 3, Melbourne VIC 3001

1800 931 678

info@afca.org.au

www.afca.org.au.

AFCA is our external dispute resolution scheme and can consider privacy complaints relating to the financial services we provide.

7 Contact us

We are committed to addressing your privacy concerns promptly and effectively. You may contact us regarding:

- questions about our privacy practices;
- requests to access or correct your information;
- privacy complaints or concerns;
- opting out of marketing communications;
- general enquiries about this policy.

Contact Information:

DB5 Advisers Pty Ltd ABN 52 661 311 539, trading as DB Advisers Pty Ltd
Australian Financial Services Licence No. 543198
Privacy Officer: Anthony Blythe
Address: PO Box 5233 Port Macquarie BC, NSW 2444
Phone: 0498 139 819
Email: pensions@dbadvisers.com.au
Website: www.dbadvisers.com.au