Bravium Privacy Policy

Version 10

Updated 26 August 2026

Bravium, 70/10 Lonsdale St, Braddon ACT 2612. Telephone 02 6152 0152.
www.bravium.com.au

Our commitment

Bravium is committed to providing you with the highest levels of client service. We recognise that your privacy is very important to you. The Privacy Act 1988 (Cth) sets out a number of Australian Privacy Principles (APPs). Our aim is to both support and ensure that we comply with these principles. Further information on privacy in Australia may be obtained by visiting the website of the Office of the Australian Information Commissioner at https://www.oaic.gov.au/.

This Privacy Policy discloses the purpose, and how the personal information you provide to us and our representatives, is collected, used, held, disclosed and disseminated.

Your personal information

As a financial service provider, Bravium is subject to certain legislative and regulatory requirements under s961B of the Corporations Act and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. These require us to obtain personal information about you including:

- your name, contact details, and date of birth;
- information regarding your dependents and family commitments, which where it is relevant to your advice or estate planning may include the names and dates of birth of your children;
- your occupation, and employment history;
- your financial needs and objectives;
- your assets, liabilities, income, expenses, insurances and social security entitlements; and
- your tax file number, and identification documents used to verify who you are.

How we collect personal information

Bravium collects personal information directly from you or from third parties once authorisation has been provided by you. You have the right to refuse us authorisation to collect such information from a third party.

Our document portal

We use a secure document portal, DoxAi, to collect documents from you and to send documents to you. When we need something such as a superannuation statement or a payslip, we send you a request and you upload the document to the portal rather than attaching it to an email. You access the portal using a code sent to your mobile telephone, so it is important that we hold a current mobile number for you. Every document you provide is reviewed by a member of our team.

Documents you provide are transferred to your client file and are removed from the portal automatically 90 days after we mark the request completed. Where the portal cannot be used, we may provide you with a secure folder instead. We ask that you do not email us documents containing sensitive information, as email is the least secure channel available to us.

We also use an online form, Jotform, to collect a preliminary summary of your financial position. It is not used for documents or identification.

Verifying your identity

We verify your identity using a specialist service, Personr. This involves checking the identification documents you provide, which is a requirement under anti-money laundering law as well as a protection for you.

Recordings and transcripts

We record and transcribe meetings we conduct with you, whether by telephone, video conference or in our office, for the purposes of compliance, training and future reference. Specifically:

- Telephone calls are transcribed to written text. We do not keep an audio recording of a telephone call, only the transcript.
- Meetings held through Microsoft Teams are recorded to video and transcribed. Teams displays an on-screen notification to everyone in the meeting while recording is running.

This policy is how we let you know that our calls and meetings are recorded and transcribed. We will not usually repeat it at the start of each call or meeting. If you would prefer that a particular conversation, or all of your conversations, are not recorded or transcribed, simply tell us and we will turn it off and take notes instead. It will not affect the advice you receive.

How we use your personal information

Primarily, your personal information is used in order to provide advice to you. We may also use the information that is related to the primary purpose and it is reasonable for you to expect the information to be disclosed.

We also keep records of our conversations with you so that we can maintain continuity in the advice relationship. Advice given over a number of years depends on our understanding what you told us earlier, what mattered to you and why a decision was made at the time. Whoever you speak to at our firm should be working from the same understanding of your circumstances.

When we may disclose your personal information

In line with modern business practices common to many financial institutions and to meet your specific needs we may disclose your personal information to the following people or organisations:

- superannuation fund trustees, insurance providers, fund managers and other product providers in order to manage or administer your product or service;
- compliance consultants to ensure we are meeting our obligations under relevant legislation;
- outsourced paraplanners;
- mailing houses;
- your professional advisers, including your solicitor or accountant as authorised by you;
- information technology providers, including but not limited to Microsoft, Salesforce, DoxAi and our managed IT provider;
- Bravium staff (unless otherwise agreed);
- a potential purchaser or organisation involved in the proposed sale of our business for the purpose of due diligence, corporate re-organisation and transfer of all or part of the assets of our business. Disclosure will be made in confidence and it will be a condition of that disclosure that no personal information will be used or disclosed by them;
- a new owner of our business that will require the transfer of your personal information; or
- government and regulatory authorities, as required or authorised by law.

Our employees and the outsourcing companies and personnel are obliged to respect the confidentiality of any personal information held by Bravium.

As members of the Financial Advice Association Australia (FAAA), we are required to meet a level of professional standards. From time to time, we may need to provide the Association with access to your personal information to ensure that we are meeting our compliance requirements.

The Corporations Act has provided the Australian Securities and Investments Commission with the authority to inspect certain personal information that is kept on our files about you.

We collect information about you for the purpose of reporting to AUSTRAC under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

How we store and protect your personal information

We store your personal information electronically. We do not maintain paper client files; anything we receive on paper is scanned to your file and the paper destroyed securely. Your information is held in our Microsoft 365 environment and in Salesforce, and documents pass through our DoxAi portal. All three store data on Australian servers. These files are accessible to authorised personnel only and are appropriately secured and subject to confidentiality requirements.

We take many steps to protect this information, including staff training, anti-virus software, password protection technology and multi-factor authentication. Access is limited to what each staff member needs in order to do their job, our systems are monitored by a managed IT provider, and our staff are bound by an internal cyber security policy which they must acknowledge in writing. In the unlikely event of a data breach we have measures in place to respond and manage these risks, including assessing whether the breach must be notified to you and to the Office of the Australian Information Commissioner.

How long we keep your information

It is a legislative requirement that we keep personal information and advice records for a period of 7 years. Should you cease to be a client of ours, we will maintain your personal information in a secure manner for 7 years, after which it will be destroyed. Records of the identity checks we carry out are kept for the same period, as anti-money laundering law requires.

Video recordings of meetings are deleted automatically after twelve months. The written transcript remains on your file as part of our advice records for the period described above.

Do we send personal information to overseas recipients?

We retain your information on Australian servers. Storing information in Australia is not the same as restricting access to it, and we think you should know where access from outside Australia occurs. At the date of this policy:

- we engage contracted staff located in the Philippines, employed through Levera, who work on client administration and support within our systems;
- one member of the support team for our document portal is located in Italy, with the remainder of that team in Sydney; and
- a software developer located in India works on our client record system.

In each case access is limited to what the work requires, those staff and contractors are bound by the same confidentiality obligations as our Australian employees, and where the work can be done without access to live client information, that is how we do it. Some of the product providers and other entities we share information with may also have operations in other countries. When information is stored or accessed overseas we make sure appropriate data handling and security arrangements are in place, and in some circumstances we may need to obtain your prior consent. We will update this policy if these arrangements change.

How do we use artificial intelligence?

We may use artificial intelligence tools to help us organise and summarise information such as meeting transcripts and client records. The tools we use are Microsoft Copilot, and Salesforce Einstein and Agentforce. Each of these forms part of the existing systems in which your information is already stored, which avoids sharing your information with third party applications. Artificial intelligence is used by Bravium solely for the purpose of our financial advice relationship with you and not for any secondary purpose.

A person is responsible for the advice we give you. Every document you provide is reviewed by a member of our team, and every piece of advice is prepared and checked by a person before it reaches you. Where an artificial intelligence tool summarises information or drafts a task, that output supports our work and is reviewed by a member of our team rather than acting on its own. If this changes, we will update this policy and tell you.

How do we ensure your personal information is correct?

Bravium takes all reasonable precautions to ensure that the personal information we collect, use and disclose is accurate, complete and up-to-date. To ensure we can maintain this level of accuracy and completeness, we recommend that you:

- inform us of any errors in your personal information; and
- update us with any changes to your personal information as soon as possible.

If you provide inaccurate or incomplete information we may not be able to provide you with the products or services you are seeking.

Using government identifiers

Although in certain circumstances we are required to collect government identifiers such as your tax file number, Medicare number or pension card number, we do not use or disclose this information other than when required or authorised by law or unless you have voluntarily consented to disclose this information to any third party.

Dealing with us anonymously

You can deal with us anonymously where it is lawful and practicable to do so. For example, if you telephone requesting our postal address.

Your sensitive information

Without your consent we will not collect information about you that reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs or affiliations, membership of a professional or trade association, membership of a trade union, details of health, disability, sexual orientation, or criminal record. Where we do collect health information, it is because it is relevant to insurance advice you have asked us to provide, and we collect it with your consent.

This is subject to some exceptions including when:

- collection is required by law; and
- the information is necessary for the establishment, exercise or defence of a legal claim.

Use of Open Banking and Consumer Data Right (CDR) data

Bravium may collect and use certain personal information through accredited Open Banking connections under Australia's Consumer Data Right (CDR) framework. The CDR is a regulated data-sharing system that allows consumers to securely share banking and other financial data with accredited service providers, only with their explicit consent. It is overseen by the Australian Competition and Consumer Commission (ACCC) and supported by the Office of the Australian Information Commissioner (OAIC) to ensure strong privacy, security and consent protections are maintained.

When you authorise us to access your banking or related financial data through an Open Banking connection, Bravium may use secure services, such as our approved CDR data provider Fiskil, to retrieve this information strictly for the purpose of delivering financial advice and related services. Under the CDR Rules, any data sharing must comply with rigorous consent standards, including clear disclosure of:

- the specific data being requested;
- the purpose for which the data will be used;
- the period for which the data may be accessed; and
- your right to withdraw consent at any time.

We handle all Open Banking data in accordance with the Australian Privacy Principles, including APP 1 (open and transparent management of personal information), APP 6 (use and disclosure), APP 10 (quality of personal information), and APP 11 (security of personal information). These principles govern the collection, use, disclosure, accuracy, access, correction and protection of your personal information.

Your CDR data is transferred using CDR-compliant secure interfaces and is protected through encryption, strict access controls and audit requirements as mandated under the CDR regime. Bravium does not access, store or use CDR data beyond what you have explicitly authorised. If you withdraw consent, data sharing will cease immediately and any active authorisations will be revoked.

Bravium will never share your CDR-sourced data with third parties except where required by law or where you have provided explicit, informed consent. All handling of CDR data is subject to the same care, security and confidentiality obligations that apply to all personal information collected under this Privacy Policy and the Privacy Act 1988 (Cth).

How can you contact us about privacy?

You can call us on 02 6152 0152, send an email to hello@bravium.com.au or write to us at PO Box 5233, Braddon ACT 2612.

How can you complain about privacy?

Please contact us if you wish to complain about any breach or potential breach of your privacy rights. We will acknowledge your complaint within 7 days and provide a final response within 30 calendar days.

If you are not satisfied with the outcome of your complaint, you may take it to an external body at no cost to you. Which body is appropriate depends on the nature of your complaint, and you are welcome to ask us if you are not sure.

The Australian Financial Complaints Authority (AFCA) considers complaints about financial services. AFCA can be contacted on 1800 931 678, at info@afca.org.au, at www.afca.org.au, or by post at GPO Box 3, Melbourne VIC 3001.

The Office of the Australian Information Commissioner (OAIC) considers complaints about the handling of personal information. The OAIC can be contacted on 1300 363 992, at www.oaic.gov.au, or by post at GPO Box 5288, Sydney NSW 2001.

How do you access your personal information?

You have a right to access your personal information, subject to certain exceptions allowed by law. We ask that you provide your request for access in writing (for security reasons) and we will provide you with access to that personal information. We will respond within 30 days. Access to the requested personal information may include:

- providing you with copies;
- providing you with the opportunity for inspection; or
- providing you with a summary.

You may also ask us to correct any personal information that is inaccurate, out of date or incomplete.

Some exceptions exist where we will not provide you with access to your personal information if:

- providing access would have an unreasonable impact on the privacy of others;
- providing access would be unlawful;
- denying access is required or authorised by or under law; or
- providing access would be likely to prejudice certain operations by or on behalf of an enforcement body, or an enforcement body requests that access not be provided on the grounds of national security.

Should we refuse you access to your personal information, we will provide you with a written explanation for that refusal and tell you how you can complain about that decision.

There is no cost to make a request for information, however in some cases there may be a charge to cover the time we spend locating and compiling the information. We will provide an estimate upfront if a charge will apply.

About this policy

This policy is effective 26 August 2026. We review it at least annually and whenever we make a material change to the systems we use. A copy of this Policy is published to our website and you may request a printed copy at any time.

Bravium Pty Ltd ABN 29 303 493 860