

Bravium Privacy Policy

Version 9

Updated 6th February 2026

Bravium
70/10 Lonsdale St,
Braddon ACT 2612
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. Privacy Amendment (Enhancing Privacy Protection) Act 2012 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;
- your occupation, and employment history;
- your financial needs and objectives; and
- your assets, liabilities, income, expenses, insurances and social security entitlements.

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. We may also record meetings we conduct with you via telephone, video conferencing or in office for the purpose of training, compliance and for reference.

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.

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 and Salesforce);
- Bravium staff (unless otherwise agreed);
- a potential purchaser/organisation involved in the proposed sale of our business for the purpose of due diligence, corporate re-organisation and transfer or 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/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.

Bravium takes its obligations to protect your personal information seriously. In some circumstances we may need to obtain your prior consent if it is likely that disclosure of personal information will be made to an overseas recipient.

How we store and protect your personal information

We store your personal information electronically and occasionally in paper based format. These files are accessible to authorised personnel only and are appropriately secured and subject to confidentiality requirements. Bravium takes its obligations to protect your personal information seriously. In this regard, information may be stored in servers or related resources that are external to Australia, however we retain information on Australian servers where possible (including our Salesforce instance and our Microsoft servers).

We take many steps to protect this information, including staff training, anti-virus software, password protection technology and multi-factor authentication. In the unlikely event of a data breach we have measures in place to respond and manage these risks.

It is a legislative requirement that we keep all personal information and records for a period of 7 years. Should you cease to be a client of ours, we will maintain your personal information on or off site in a secure manner for 7 years. After this, the information will be destroyed.

Do we send personal information to overseas recipients?

Some of the entities that we share information with may be located in, or have operations in, other countries. This means your information may be stored or accessed in overseas countries such as the Philippines and the United States. When information is stored or accessed overseas we make sure appropriate data handling and security arrangements are in place.

How do we use Artificial intelligence?

We may use artificial intelligence tools to analyse information such as meeting recordings and client data. The tools used are Microsoft Co-pilot and Salesforce Einstein, being part of the existing systems we use to store your information, and therefore removing the risk of sharing information

with 3rd party applications. Artificial Intelligence is used by Bravium solely for the purpose of our financial advice relationship with you and not for any secondary purposes.

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 professional or trade association, membership or a trade union, details of health, disability, sexual orientation, or criminal record.

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. Your complaint will be responded to within 7 days. If you are not satisfied with the outcome of your complaint, you are entitled to contact the Office of the Privacy Commissioner.

We can be contacted using any of the above mentioned contact channels.

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. 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.

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;
- 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.

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 6th February 2026. We will update this policy as changes to our business occur. A copy of this Policy is published to our website and you may request a printed copy at any time.