

Privacy Policy

September 2026

Table of Contents

1. Respecting your privacy	3
2. Terminology	3
3. How do we collect your personal information?	4
4. How do we store your personal information?	5
5. Why do we collect your personal information?	5
6. How do we use and disclose your personal information?	6
7. How do we protect your personal information?	6
8. Destruction of your personal information	7
9. Access to and correction of your personal information	7
10. Complaints	7
11. Data breach notification requirements	8
12. Privacy contact details	8
13. Updates to our Privacy Policy	8

1. Respecting your privacy

Frontier Advisors Pty Ltd ACN 074 287 406 (Frontier) of Level 17, 130 Lonsdale Street, Melbourne, Victoria, Australia 3000, and our subsidiaries and related bodies corporate ('we', 'our' and 'us') are committed to complying with the Privacy Act 1988 (Cth) (Privacy Act) and the Australian Privacy Principles (APPs) that apply to our handling of personal information. Our respect for your right to privacy of your personal information is paramount. We take privacy seriously and maintain measures designed to ensure personal information is handled appropriately, regardless of how or where it is collected.

Personal information forms part of Frontier's broader information governance framework arrangements and is managed in accordance with Frontier's Information Security Policy, Information Classification, Handling & Lifecycle Management Standard, Identity & Access Management Standard and other applicable governance and control documents. Frontier applies reasonable technical, organisational and operational safeguards to protect personal information throughout its lifecycle.

This Privacy Policy sets out:

- matters of which you should be aware regarding information we may collect about you
- our policies on the management of your personal information
- generally, what sort of information we hold, why we hold the information we hold, and how we collect, hold, use and disclose that information.

You may not provide us with personal information, or you may deal with us on an anonymous or pseudonymous basis. However, this may restrict our ability to provide our services to you or to otherwise deal with you (including responding to requests for access to or correction of your personal information or responding to a complaint).

We may provide additional privacy notices when collecting personal information for a particular service, portal, event, recruitment process or other activity. Any additional notice should be read together with this Privacy Policy.

2. Terminology

In our Privacy Policy, "personal information" refers to information or an opinion about an identified person or a person who is reasonably identifiable from the information or opinion.

"Sensitive information" is a category of personal information that receives additional protection under the Privacy Act. We collect sensitive information only where it is reasonably necessary for our functions or activities and where we have consent or another lawful basis to do so.

3. How do we collect your personal information?

In accordance with the APPs, we only collect personal information about an individual if the information is necessary for one or more of our functions or activities and we must only collect personal information by lawful and fair means. Further, we must not collect personal information in an unreasonably intrusive manner. If it is reasonable and practicable to do so, we will collect personal information about an individual only from that individual. However, we comply with the APPs by taking reasonable steps to make an individual aware of the matters outlined in our Privacy Policy, even where we collect the personal information about an individual from someone else.

We may collect your personal information directly from you, or alternatively, where permitted under the APPs, from third parties. Sources may include, but are not limited to:

- your employer in the case of being authorised to use our Partners Platform online portal
- Partners Platform online portal usage data
- a telephone or in-person enquiry about our services
- emails or other electronic means (including by using our website)
- third parties, such as credit reporting agencies or your representatives
- publicly available sources of information
- our service providers
- client onboarding, due diligence and service delivery activities
- use of Frontier client portals, reporting solutions and digital services
- investment consulting, implemented consulting and portfolio management activities
- attendance at Frontier events, webinars and training sessions
- recruitment and employment-related activities.

The types of personal information we may collect include but may not be limited to your name, address, telephone number, email address and photographs.

When you use our website, portals, emails or other digital services, we may collect technical and usage information such as your IP address, device and browser information, access dates and times, referring domains, pages viewed, links selected and service activity. Some of this information may constitute personal information or may become identifiable when combined with other information.

We may use cookies and similar technologies to operate our digital services, remember preferences, understand how our services are used, improve performance and maintain security. You may be able to control cookies through your browser or an available cookie-preference tool. Disabling some cookies may affect the operation of parts of our website or digital services.

Our website or electronic communications may also use analytics technologies or tracking pixels to help us understand how digital services and communications are used.

4. How do we store your personal information?

We hold personal information using a combination of approved technology platforms, physical records, systems and service providers. Personal information may be stored or processed in Australia or overseas, depending on the services and providers involved.

We take reasonable technical, organisational and operational steps to protect personal information against misuse, interference, loss, and unauthorised access, modification or disclosure. The measures applied depend on the nature and sensitivity of the information, how it was collected, the way it is used and the environment in which it is held.

We retain personal information only for as long as reasonably necessary for the purposes for which it was collected and to satisfy applicable legal, regulatory, contractual, audit, dispute and record-keeping requirements.

5. Why do we collect your personal information?

We may collect personal information for one or more of the following purposes:

- to provide our services to you or to other persons or organisations that are related to you
- to provide you or any other person or organisation related to you with access to our online portal
- to market, advertise or otherwise promote our services
- to undertake market research in relation to our services
- to improve our website, our online portal and our online services
- to comply with our obligations under any applicable laws.

We may need your personal information to notify you of future improvements to our services or to seek your participation (purely on a voluntary basis) in advertising campaigns, launches, customer testimonials and focus groups.

Generally, you have no obligation to provide any information we request (except under any contract between you or your related party and us where you may be obliged to provide information). If you choose to withhold requested information, however, we may be unable to provide you or other persons or organisations that are related to you, or which you represent, with the services that depend on our collection of your personal information (particularly if the collection of that information is required by law).

Where we use your personal information to directly market ourselves or our services to you and we collected this information directly from you, we will use your personal information to directly market to you where you would reasonably expect us to use your personal information for that purpose. Where we collect your personal information from other sources, we will first obtain your consent in accordance with the Privacy Act.

Frontier may use approved technology, automation and artificial intelligence-enabled tools to support business operations, service delivery, reporting, analysis and administrative activities. Where these technologies are used, they remain subject to Frontier's privacy, confidentiality, information security and governance requirements. Frontier personnel remain accountable for decisions and outputs produced with the assistance of these technologies.

6. How do we use and disclose your personal information?

We generally use your personal information to provide goods or services to you or to other persons or organisations related to you or which you represent. For example, we need your contact details to provide you with access to our investment advisory services (including via our online portal).

We may disclose your personal information to third parties (including credit reporting agencies, banks and our professional advisers) for the purpose of completing our obligation owed to you or any entity associated with you under any contract between us and you or such entity, as required by law.

Some service providers, technology providers, business partners and professional advisers that support Frontier may be located outside Australia or may store or process personal information outside Australia. Where Frontier discloses personal information to an overseas recipient, Frontier takes reasonable steps required by the Privacy Act to ensure the recipient handles the information consistently with applicable Australian privacy requirements, unless an exception applies.

You may contact us for further information about the countries in which overseas recipients are likely to be located. The countries involved may change as Frontier's services and providers change.

We may use or disclose your personal information for the purpose of directly marketing our services to you. Where required, our marketing communications will include a method for unsubscribing or opting out. You may also ask us at any time not to use or disclose your personal information for direct marketing by contacting us using the details in this Policy.

We may use your personal information for the purpose of verifying your identity and responding to your requests for access to and/or correction of your personal information we hold and responding to and handling any complaints you may have regarding our use and/or disclosure of your information.

You have the right to tell us you do not want us to send information to you other than for the main purpose for which we collect your personal information. Where possible, we try to ensure our disclosure of your personal information to other organisations is provided in a way which does not personally identify individuals.

7. How do we protect your personal information?

We take reasonable steps to protect your personal information which we hold, from misuse and loss and from unauthorised access, modification or disclosure.

When using our website or our online portal, you should be aware that no data transmission over the internet can be guaranteed to be completely secure. Although Frontier uses reasonable safeguards, no method of internet transmission or electronic storage can be guaranteed to be completely secure. You should take appropriate care when providing information electronically and contact Frontier promptly if you believe information has been transmitted, accessed or disclosed insecurely.

8. Destruction of your personal information

When personal information is no longer required, Frontier takes reasonable steps to securely destroy or permanently de-identify it, unless its retention is required or permitted by law.

9. Access to and correction of your personal information

In accordance with the APPs, we will provide you with access to any of your personal information we hold, unless the request is unreasonable or the Privacy Act or the APPs permit or require us to decline that request. If you wish to access or correct personal information we hold about you, please contact us using the details set out in Section 12 of this Privacy Policy.

If you need to update your information (for example, if you change your address), please contact us so that we can make the change. You may also request that we correct personal information you believe is inaccurate, out of date, incomplete, irrelevant or misleading.

We may need to verify your identity before responding to an access or correction request. In circumstances where we decline access to, or the correction of, your personal information, where required, we will provide written reasons for the decision and information about available complaint options.

We will not charge you for making an access or correction request. However, we may charge a reasonable amount for providing access where permitted by law and will advise you of any proposed charge before proceeding.

10. Complaints

If you wish to make a complaint about an alleged breach of your privacy or an alleged breach of the APPs, the complaint should be made using the contact details set out in Section 12 of this Privacy Policy.

Receipt of your complaint will be acknowledged and we will endeavour to deal with your complaint and provide you a response within a reasonable time (which in most situations will be within 30 days of our receipt of your complaint). Where a matter requires a more detailed investigation, it may take longer to resolve. We will provide you with progress updates if this is the case and may seek further information from you.

Where required by the Privacy Act, we will provide written acknowledgment of your complaint and information on how we will deal with your complaint. Further, where we are required to do so by the Privacy Act, we will provide you our determination on your complaint in writing.

In limited circumstances, Frontier may decline to investigate a complaint further where it is frivolous or vexatious, or where the matter has already been adequately considered. Where appropriate, we will explain the basis for the decision and any available review options. If you are dissatisfied with the outcome of your complaint, you may seek internal review of the decision. Internal review will be conducted by an officer who has not previously been involved in your complaint.

If you remain dissatisfied after Frontier has considered your complaint, you may contact the Office of the Australian Information Commissioner. If another external dispute resolution scheme applies to the particular matter, we will provide relevant details where appropriate.

11. Data breach notification requirements

The Privacy Act requires us to report "eligible data breaches" to the Office of the Australian Information Commissioner and to affected individuals.

An "eligible data breach" occurs if there is unauthorised access to, or disclosure of, information we collect and a reasonable person would conclude such access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates. "Serious harm", while undefined, is likely to include serious physical, psychological, emotional, economic, or financial harm, or serious harm to reputation.

An exception applies when remedial action is taken to prevent serious harm to any affected individual before the individual suffers the harm. If the breach applies to multiple entities, only one entity must notify the Office of the Australian Information Commissioner and affected individuals for all entities. Reporting is not required if it would be likely to prejudice law enforcement related activity or would be inconsistent with a secrecy provision.

We must take reasonable steps to notify affected individuals of the breach, such as via email, telephone or post. However, if we determine it is not practicable to notify affected individuals directly, then we must publish a statement on our website and take reasonable steps to publicise the statement.

12. Privacy contact details

Privacy enquiries, access and correction requests, complaints and suspected privacy breaches may be submitted to:

Frontier Advisors Risk and Compliance

Email: riskandcompliance@frontieradvisors.com.au

Postal address:

Frontier Advisors Pty Ltd
Level 17, 130 Lonsdale Street
Melbourne VIC 3000

13. Updates to our Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our activities, practices, services, technology or legal obligations. The current version will be published on our website and will identify the date on which it was last updated. You may obtain a copy of the current Privacy Policy from our website or by contacting us.