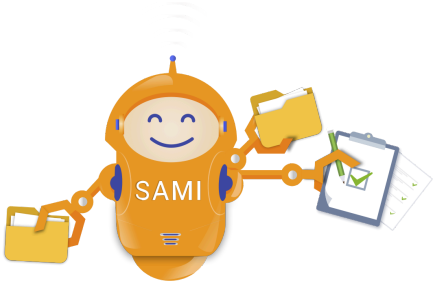
advice REGTECH



Advice RegTech -

Privacy Policy

Version 26.11.10

Last updated 10 November 2026

Table of Contents

Privacy Policy 1
Advice RegTech Privacy Policy 3
- Overview 3
- Our Privacy Governance 3
- What Personal Information Do We Collect? 3
  - A. Public website visitor information 3
  - B. Job applicant and contractor information 4
  - C. SaaS application information 4
  - D. Client data we process on behalf of our Clients 4
- How Do We Collect Personal Information? 5
- Sensitive Information 5
- How Do We Use The Personal Information We Collect? 6
- Automated Decision-Making 6
- Disclosure of Personal Information 7
- Cross-Border Disclosure of Personal Information 8
- How Do We Store and Protect Personal Information? 8
- Retention and Return of Personal Information 8
- Data Breach and Security Incident Notification 9
- Cooperation with Client Audits and Regulatory Requests 9
- Rights 9
- Changes to the Privacy Policy 10
- Contact 10

Public Website - Internet Privacy Policy 11
- Personal Information 11
- Use of Information 11
- Collecting Information on Registered Members and Enquiries 11
- Disclosure 12
- Security 12
- Collecting Information from Visitors 12
- Access to Information 12
- Links to Other Sites 13
- Problems or Questions 13
- Changes to the Privacy Policy 13

Advice RegTech Privacy Policy

Overview

Advice RegTech Pty Ltd ABN 21 617 175 710 (‘Advice RegTech’, ‘we’, ‘us’ or ‘our’) is fully committed to maintaining client confidentiality and privacy. In order to promote transparency and ensure confidence in how personal information is being used within Advice RegTech, this Privacy Policy outlines what personal information we store, how we use personal information, and other specific details relating to personal information. Throughout this Privacy Policy we refer to ‘personal information’, which means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not it is true and whether or not it is recorded in a material form. We also refer to ‘you’ as the person whose personal information we collect and hold.
Where we refer to a ‘Client’, we mean the business that has contracted with us to use our SaaS application — typically an Australian Financial Services Licensee (AFSL), superannuation trustee, insurer or other APRA-regulated or licensed financial services business. Where we refer to a ‘User’, we mean an individual — typically an employee or authorised representative of a Client — who accesses the SaaS application on the Client's behalf. Where we refer to an ‘End Customer’, we mean an individual who is a customer or member of our Client (for example, a financial adviser's client, or a superannuation fund member), whose personal information may appear in files a Client uploads to our SaaS application for compliance review or record-keeping. This distinction matters because our obligations differ depending on whose personal information is involved — see 'Client data we process on behalf of our Clients' below.

Our Privacy Governance

We are committed to complying with the Australian Privacy Principles (APPs) in the Privacy Act 1988 (Cth), and to being accountable for the way we handle personal information. We maintain internal practices, procedures and systems designed to embed privacy considerations into our SaaS application, respond effectively to privacy enquiries and complaints, and support our Clients' own regulatory obligations. We review these practices regularly, including as our products, services and use of technology, such as AI-enabled features, evolve.

What Personal Information Do We Collect?

Advice RegTech collects personal information from its: website visitors; job applicants and contractors; SaaS application Clients and Users; and the End Customers of our Clients. The types of personal information that we collect includes only necessary information for the relevant function or activity.

A. Public website visitor information

for the purpose of responding to enquiries and tracking cookies for visitor interest in areas of our public website. Contact form information collected includes:

- Name

- Email
- Company
- Phone
- Comment.

Please see our Internet Privacy Policy attached.

B. Job applicant and contractor information

for the purpose of assessing applications for employment, conducting pre-employment background checks, and engaging and paying contractors:

- Name and contact details (address, email and phone);
- Résumé, qualifications, employment history and referee reports;
- Background check results, which may include police checks, collected only with consent;
- For contractors, business and payment details (such as ABN and bank account details).

C. SaaS application information

for the purpose of Users being able to access and use the SaaS application:

- Full name;
- Work email address;
- Mobile phone number;
- Employer / company name and business address;
- User ID / account identifier;
- Work role and permissions.

The SaaS application handles items from Clients / Users for compliance reviews and record keeping, which may contain other personal information, including personal information about a Client's End Customers. See 'How do we store and protect personal information' for information on the multiple levels of security in place and how we take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

D. Client data we process on behalf of our Clients

for the purpose of enabling our Clients to conduct compliance assurance activities, including advice file reviews and record-keeping, using our SaaS application.

Our SaaS application allows Clients to upload files (such as financial advice files and audio files) for compliance review, service quality review, and for record-keeping evidence of supervision and monitoring. These files may contain personal information — including sensitive information such as health information, about a Client's End Customers.

We collect, hold, use and disclose this personal information solely as a service provider acting on behalf of, and under the instructions of, our Client, for the purpose of providing our SaaS application and the compliance review and record-keeping services our Client has engaged us to provide. We do not use End Customers' personal information for our own independent purposes — for example, we do not use it for direct marketing, and (other than

as described under 'Automated Decision-Making' below) we do not use it to develop our artificial intelligence or machine learning models.

The primary privacy relationship for an End Customer remains with our Client, who is generally responsible for collecting that individual's personal information and for their own privacy obligations as an APP entity. If you are an End Customer and have a question about how your personal information is being handled, we recommend you contact the Client (for example, your financial adviser, licensee or superannuation trustee) in the first instance. Our Client can then engage us as needed to assist in responding to your query.

How Do We Collect Personal Information?

Where it is reasonably practical to do so, we will collect your personal information directly from you. We may collect personal information through some of the following means:

- from any person nominated by you, including solicitors, accountants and financial planners or their Australian Financial Services Licensees (AFSL);
- in the course of administering or providing any of our services, including when you provide us with information verbally, or complete and submit written forms;
- when you access and use our SaaS application, website, subscribe to our email service, or social media;
- when you communicate with us via telephone, email, or otherwise correspond with us (whether in writing or electronically);
- in the course of administering, performing or managing contracts with our service receivers, service providers or other third parties;
- from a Client, where the information relates to that Client's End Customer and has been uploaded to our SaaS application for compliance review or record-keeping;
- when you provide us with information in response to direct marketing or customer satisfaction and market research surveys and questionnaires;
- when you apply for employment with us; and
- as otherwise required to manage our business.

You have no obligation to provide any personal information requested by us. However, if you choose to withhold personal information, we may not be able to provide you with certain parts of our products or services. Where it is lawful and practicable, you may deal with us anonymously or under a pseudonym — for example, when making a general enquiry about our products or services. In most other circumstances, we will need to identify you in order to provide our products and services, administer a Client's advice file, verify your identity, or comply with our legal and regulatory obligations, and we may not be able to assist you if you choose not to identify yourself.

Sensitive Information

Some of the personal information we handle — particularly within advice files uploaded to our SaaS application for compliance review — may be 'sensitive information' under the Privacy Act 1988 (Cth), such as health information or information about an individual's racial or ethnic origin. Sensitive information is subject to a higher standard of protection under the Australian Privacy Principles (APPs). We only collect, use, handle and disclose sensitive

information as reasonably necessary for the purposes described in this Privacy Policy, in accordance with a Client's instructions (where applicable), or as otherwise permitted or required by law. We do not require Tax File Numbers to provide our services. If a Tax File Number is provided to us, we will handle it in accordance with our legal obligations.

How Do We Use The Personal Information We Collect?

We use the personal information that we collect to supply our products and services. In particular, we may collect, hold, use and disclose personal information:

- to offer and provide our products and services, or request feedback about products and services received;
- to manage and administer those products and services;
- for direct marketing purposes, including to prepare and provide marketing information about our products and services and those of our related companies and other organisations in accordance with the Privacy Act 1988 (Cth) — this does not apply to personal information we hold about a Client's End Customers, which we do not use for direct marketing;
- to conduct business planning and research, including analysing general statistical information regarding the use of our website and SaaS application;
- to communicate with you;
- to comply with our legal and regulatory obligations;
- for any purpose disclosed to you and to which you have consented;
- for any purpose that you would otherwise reasonably expect; and
- otherwise to appropriately manage and conduct our business, including performing administrative functions such as billing, accounts, user management and records management.

Automated Decision-Making

Our SaaS application includes optional AI-enabled features that assist Users in reviewing items uploaded to the application. These AI features are only activated at a Client's request and can be switched off by the Client at any time.

Our third-party AI service providers do not use personal information to train or fine-tune their underlying models. Some Advice RegTech features may, in limited circumstances, use personal information to tailor functionality to a Client's specific requirements. Where this occurs, the Client may elect to opt out of that use, and we will not use its End Customers' personal information for that purpose.

Our Clients may use these AI features to help their compliance professionals make decisions that could significantly affect individuals. These include risk scoring of financial advisers, paraplanners and call centre operators for coaching and quality assurance, and identifying End Customers who may need human review, corrective or remedial action. The AI features may influence those decisions even though a person, not our application, makes the final determination. For that reason, we set out below the categories of personal information used and the types of decisions involved.

Categories of personal information used by these computer programs:

- identity and contact information about End Customers, financial advisers, paraplanners, general advice providers and call centre operators;
- financial information recorded in advice documents, including income, assets, liabilities, objectives and needs;
- health information, where it is included in advice documents (for example, for insurance advice);
- audio recordings of calls and their transcripts; and
- information about the advice provided, including file notes, statements of advice and records of adviser conduct.

Types of decisions for which these computer programs do a thing substantially and directly related to making the decision:

- assessing whether files show indications of non-compliance with Client-specified regulatory and licensee obligations;
- identifying potential breaches, risks or service-quality issues in files;
- identifying files that may require further review or remediation for an End Customer; and
- informing assessments of a financial adviser's and general advice provider's compliance.

Decisions made solely by these computer programs: none. Our application does not itself record a final determination about an individual; that determination is made by our Client. Our Clients decide how they use the outputs of our AI features and are responsible for the decisions they make. We provide Clients with information about our AI features to help them meet their own privacy obligations, and further information is available to Clients on request. We will review this section if the categories of personal information used, or the types of decisions supported, change.

Disclosure of Personal Information

Advice RegTech will never disclose or share personal information obtained from its Clients, End Customers, website visitors, Users or job applicants / contractors with other people or organisations, except for:

- our Clients, in relation to personal information we hold on their behalf and information about their Users;
- our contractors, suppliers, partners, service providers (including organisations that provide us with technical and support services);
- our professional advisors, auditors or consultants, where permitted by the Privacy Act 1988 (Cth); and
- where you have consented, or where disclosure is required or authorised by law (for example, to a regulator, court or law enforcement body).

If we disclose information to a third party, we generally require that the third party protect that information to the same extent that we do.

Cross-Border Disclosure of Personal Information

Our SaaS application and the personal information we hold within it, are hosted in Australia with an established cloud service provider. Data is stored in Australian Data Centres. Some data processing may occur outside Australia, when approved in advance by our Clients.

We also engage a small number of specialist third-party service providers to support specific functions of our application, such as network security, two-factor authentication and outbound email, which may involve limited categories of personal information (such as a phone number or email address) being handled by those providers in other countries, in the course of delivering those services.

Where we disclose personal information to an overseas recipient, we take reasonable steps to ensure that the recipient handles the information consistently with the Australian Privacy Principles, in accordance with Australian Privacy Principle 8. We maintain a current list of our material sub-processors and their locations, available to Clients on request, to support Clients' own regulatory disclosure obligations, including under APRA prudential standards.

How Do We Store and Protect Personal Information?

Advice RegTech has multiple levels of security in place and takes reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Advice RegTech is ISO 27001 certified, reflecting independently audited information security management practices. Personal information in our SaaS application is stored in encrypted cloud-based data centres within Australia that require two-factor authentication in order to access. Personal information is encrypted in transit and at rest using industry-standard encryption. No personal information is stored in physical format. Only employees whose work function specifically requires the use of personal information are authorised to access the personal information. Employees are required to sign nondisclosure agreements prior to handling personal information. For a comprehensive listing of firm information security procedures, a copy of the Advice RegTech Information Security Policies and Procedures (including our ISO 27001 certification) is available upon request.

Retention and Return of Personal Information

We retain personal information only for as long as reasonably necessary for the purposes for which it was collected, or as required by law or by our contractual arrangements with our Clients. This may include retention periods of 7 years or more, consistent with a Client's own regulatory record-keeping obligations (for example, under the Corporations Act 2001 (Cth) or APRA prudential standards). We destroy or de-identify personal information that we no longer need, subject to any such legal or contractual retention requirement.

Upon expiry or termination of our agreement with a Client, we will return and/or securely destroy that Client's personal information and its End Customers' personal information in accordance with our agreement with that Client, unless we are required by law to retain it.

Where a Client requests removal of personal information from our application, we delete data in accordance with our agreement with that Client. Residual copies held in backups and system logs (for example, user access records) are retained for limited periods for security and audit purposes before being permanently removed.

Data Breach and Security Incident Notification

In the event of an eligible data breach involving personal information, we will comply with our obligations under the Notifiable Data Breaches scheme in the Privacy Act 1988 (Cth), including notifying the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable, and notifying any other governmental authority as required by law.

Where a security incident affects personal information we hold on behalf of a Client, we will notify that Client in accordance with our agreement with them, which includes notification commitments designed to support the Client's own regulatory obligations, including under APRA Prudential Standard CPS 234.

Cooperation with Client Audits and Regulatory Requests

Where required under our agreement with a Client, we will reasonably cooperate with audits, information requests and regulatory inquiries relating to the personal information we handle on that Client's behalf, including those made by or on behalf of APRA in connection with a Client's outsourcing or material service provider arrangements with us.

Rights

Please contact our Privacy Officer using the details below if you wish to:

- withdraw your consent to our usage of your personal information at any time;
- request a copy of the personal information about you that we store; or
- request that incorrectly recorded personal information be rectified.

We are not obliged to correct any of your personal information if we do not agree that it requires correction and we may refuse to do so. If we refuse a request for access or correction, we will provide you with a written notice stating our reasons for refusing. We will respond to any request regarding your personal information within 30 days of receiving the request. We may seek to recover reasonable costs incurred in providing you with access to the personal information we hold about you.
If you wish to make a complaint about how we have handled your personal information, please contact our Privacy Officer using the details in the 'Contact' section below. We will acknowledge your complaint within 5 business days of receiving it, and aim to investigate and resolve it within 30 days.

You may lodge a complaint about our collection, storage and use of your personal information with the Office of the Australian Information Commissioner (OAIC), Australia's independent privacy regulator, at www.oaic.gov.au.

If you are an End Customer of one of our Clients, we recommend you raise privacy queries or complaints with that Client in the first instance, as described under 'Client data we process on behalf of our Clients' above.

Changes to the Privacy Policy

We will review this Privacy Policy periodically and we may update it at any time, making this accessible to Clients on the Advice RegTech SAMI Help Centre.

Contact

Any questions regarding the Advice RegTech Privacy Policy or the usage of personal information within the firm can be directed towards the Privacy Officer at the email privacy@adviceregtech.com. Advice RegTech registered office is Suite 204, 110 Pacific Highway, North Sydney, NSW, 2060.

This document was last updated on 10 November 2026.

Public Website - Internet Privacy Policy

This web site is owned and operated by Advice RegTech Pty Ltd and will be referred to as “We”, “our” and “us” in this Internet Privacy Policy. This Internet Privacy Policy, set out on this web site page, applies to your use of this web site (“the web site”).

The Internet Privacy Policy relates to the collection and use of personal information you may supply to us through your conduct on the web site. We reserve the right, at our discretion, to modify or remove portions of this Internet Privacy Policy at any time. This Internet Privacy Policy is in addition to any other terms and conditions applicable to the web site. We do not make any representations about third party web sites that may be linked to the web site. We recognise the importance of protecting the privacy of information collected about visitors to our web site, in particular information that is capable of identifying an individual (“personal information”). This Internet Privacy Policy governs the manner in which your personal information, obtained through the web site, will be dealt with. This Internet Privacy Policy should be reviewed periodically so that you are updated on any changes. We welcome your comments and feedback.

Personal Information

1. Personal information about visitors to our site is collected only when knowingly and voluntarily submitted. For example, we may need to collect such information to provide you with further services or to answer or forward any requests or enquiries. It is our intention that this policy will protect your personal information from being dealt with in any way that is inconsistent with applicable privacy laws in Australia.

Use of Information

2. Personal information that visitors submit to our site is used only for the purpose for which it is submitted or for such other secondary purposes that are related to the primary purpose, unless we disclose other uses in this Internet Privacy Policy or at the time of collection. Copies of correspondence sent from the web site, that may contain personal information, are stored as archives for record-keeping and back-up purposes only.

Collecting Information on Registered Members and Enquiries

3. As part of registering with us, or making an enquiry, we collect personal information about you in order for you to take full advantage of our services or to respond to your enquiry. Registration and enquiries are completely optional. They may include submitting your name, email address, address, telephone number, your preference on receiving updates and promotional material, and other information. You may access this information at any time by contacting us at privacy@adviceregtech.com.

Disclosure

4. Apart from where you have consented or disclosure is necessary to achieve the purpose for which it was submitted, personal information may be disclosed in special situations where we have reason to believe that doing so is necessary to identify, contact or bring legal action against anyone damaging, injuring, or interfering (intentionally or unintentionally) with our rights or property, users, or anyone else who could be harmed by such activities. Also, we may disclose personal information when we believe in good faith that the law requires disclosure.

5. We may engage third parties to provide you with goods or services on our behalf. In that circumstance, we may disclose your personal information to those third parties in order to meet your request for goods or services.

Security

6. We strive to ensure the security, integrity and privacy of personal information submitted to our sites, and we review and update our security measures in light of current technologies. Unfortunately, no data transmission over the Internet can be guaranteed to be totally secure.

7. However, we will endeavour to take all reasonable steps to protect the personal information you may transmit to us or from our online products and services. Once we do receive your transmission, we will also make our best efforts to ensure its security on our systems.

8. In addition, our employees and the contractors who provide services related to our information systems are obliged to respect the confidentiality of any personal information held by us.

Collecting Information from Visitors

9. Cookies. We use cookies to provide you with a better experience. These cookies allow us to increase your security by storing your session ID and are a way of monitoring single user access. We also use analytics cookies to understand visitor interest in areas of our web site. This information is generally collated in aggregate form and provided to us to assist in analysing the usage of the site.

Access to Information

10. We will endeavour to take all reasonable steps to keep secure any information which we hold about you, and to keep this information accurate and up to date. If, at any time, you discover that information held about you is incorrect, you may contact us to have the information corrected.

Links to Other Sites

11. We provide links to Web sites outside of our web sites, as well as to third party Web sites. These linked sites are not under our control, and we cannot accept responsibility for the conduct of companies linked to our website. Before disclosing your personal information on any other website, we advise you to examine the terms and conditions of using that Web site and its privacy statement.

Problems or Questions

12. If we become aware of any ongoing concerns or problems with our web sites, we will take these issues seriously and work to address these concerns. If you have any further queries relating to our Privacy Policy, or you have a problem or complaint, please contact us. Any questions regarding the Advice RegTech Privacy Policy or the usage of personal information within the firm can be directed towards the Privacy Officer at the email privacy@adviceregtech.com. Advice RegTech's office address is Suite 204, 110 Pacific Highway, North Sydney, NSW, 2060.

13. For more information about privacy issues in Australia and protecting your privacy, visit the Office of the Australian Information Commissioner's (OAIC) website: www.oaic.gov.au.

Changes to the Privacy Policy

This Internet Privacy Policy was last updated 10 November 2026, as was the Advice RegTech Privacy Policy attached. We will review the Privacy Policy/ies periodically and we may update them at any time by posting the new terms of the Privacy Policy on our website. Please periodically check our Privacy Policy to ensure you are aware of any recent updates: https://adviceregtech.com/privacy-policy.