advicelab

Privacy and Data Protection Statement

For Financial Adviser clients | November 2026

1. About this statement

This statement explains how Advice Lab, including its Advice Intel operations (together, "Advice Lab"), protects the personal information of your clients when we provide paraplanning and financial administration services to you. It summarises our internal Privacy and Personal Data Protection Policy, which forms part of our ISO 27001:2022 certified Information Security Management System (ISMS).

2. Our role

Advice Lab acts as a service provider to Financial Advisers and accounting firms. We do not collect personal information directly from your clients for our own purposes. We receive and handle it only to deliver the services you instruct us to provide.

- We use and disclose client information only for the services you have instructed, unless required by law.
- We never use client information for our own marketing.
- Client datasets are kept logically separate from one another.

3. Legal and regulatory framework

Our handling of client information is governed by:

- **Privacy Act 1988 (Cth)** and the Australian Privacy Principles (APPs), as amended by the Privacy and Other Legislation Amendment Act 2024 (Cth). This includes APP 6 (use and disclosure), APP 8 (cross-border disclosure) and APP 11 (security of personal information).
- **Personal Data Protection Act, No. 9 of 2022** (Sri Lanka) and the **Data Privacy Act of 2012 (RA 10173)** (Philippines), in respect of our delivery centres.
- **ISO/IEC 27001:2022 certification**, which is independently audited.

Where we use automated decision-making that could significantly affect individuals, we will meet the APP 1 transparency requirements that commence on 10 December 2026.

4. Offshore delivery

Our services are delivered by teams in Colombo, Sri Lanka and Manila, Philippines. To protect client information handled by these teams:

- Client information is held centrally in our Microsoft 365 environment, not on local systems in the delivery centres.
- It can only be accessed from company-managed, encrypted devices protected by multi-factor authentication and Conditional Access.
- Staff are bound by confidentiality obligations and our information security policies.
- Advice Lab remains accountable under the Privacy Act for client information handled by our offshore teams.

5. Security safeguards

Our key controls include role-based access, encryption of data in transit and at rest, endpoint protection and monitoring, blocking of USB storage, centralised security monitoring, prompt removal of access when staff leave, and regular backups. More detail is available in our security questionnaire responses on request.

ADVICE LAB – CONFIDENTIAL

6. Sub-processors

We use a small number of established technology providers to support our services, including Microsoft (Microsoft 365), Veeam (backup), LastPass (password management), Zoom (communications) and Amazon Web Services (cloud infrastructure). They are bound by contractual data protection obligations, and Advice Lab remains responsible to you for their handling of your client information.

7. Data breaches

If we identify a data breach involving your client information, we will contain it immediately and notify you promptly, so that you can assess it and meet your notification obligations to the OAIC and affected individuals under the Notifiable Data Breaches scheme. We will give you the information and assistance you need to do so.

8. Retention and return of data

We keep client information only for as long as needed to provide our services or as you instruct. When our services end, we securely delete or return client information.

9. Review and contact

This statement is reviewed annually, or sooner if our arrangements or the law change. If you have questions about how we handle your client information, please contact our Privacy Officer at [email address].

ADVICE LAB – CONFIDENTIAL