Privacy Policy

How Adoptic collects, holds, uses, and discloses Personal Information

[ADOPTIC PTY LTD]

ABN [XX XXX XXX XXX]

Version 1.0 — [DATE]

Confidential

Contents

1. About This Policy

This Privacy Policy explains how [Adoptic Pty Ltd] ("Adoptic", "we", "us", "our") collects, holds, uses, and discloses Personal Information. It applies to all users of the Adoptic platform at adoptic.online, including client administrators, assessors, applicants, and visitors.

Adoptic is bound by the Australian Privacy Principles ("APPs") contained in the Privacy Act 1988 (Cth). Where we handle information relating to individuals in the United Kingdom or European Economic Area, we also comply with the UK General Data Protection Regulation ("UK GDPR") and the EU General Data Protection Regulation ("EU GDPR").

By accessing or using our platform, you acknowledge that you have read and understood this Privacy Policy.

2. Definitions

Term	Meaning
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not (as defined in the Privacy Act 1988). Under GDPR, this corresponds to "personal data".
Sensitive Information	A subset of Personal Information including health information, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal records, biometric data, and trade union membership. Under GDPR, this corresponds to "special category data".
Client Data	All data uploaded to, submitted through, or generated within the platform on behalf of a client organisation, including application data, assessment data, uploaded documents, and report outputs.
Derived Data	Data produced by Adoptic's proprietary algorithms and analytical processes from Client Data, including scores, rankings, statistical summaries, and report outputs.
Aggregated Data	Data that has been combined across multiple sources and de-identified such that no individual is reasonably identifiable.
Platform	The Adoptic web application at adoptic.online and any associated APIs, tools, or services.
Data Controller	The entity that determines the purposes and means of processing Personal Information (typically the client organisation).

Term	Meaning
Data Processor	The entity that processes Personal Information on behalf of the Data Controller (Adoptic, when processing Client Data).
AI Processing	The processing of Client Data using third-party large language models (LLMs) via Amazon Bedrock to perform assessment analysis, scoring, and report generation as part of Adoptic's analytical pipeline.

3. Our Role: Data Controller vs. Data Processor

Adoptic operates in two capacities:

As a Data Processor: When we process Client Data on behalf of our client organisations (the Data Controllers). This includes storing application data, running assessments, generating reports, and hosting uploaded documents. In this capacity, we process Personal Information only in accordance with our clients' instructions and applicable law.

As a Data Controller: When we collect and process Personal Information for our own purposes, such as managing user accounts, administering the platform, communicating with users, and improving our services.

Where we act as a Data Processor, the client organisation remains responsible for ensuring that it has appropriate lawful bases and privacy notices in place for the Personal Information it collects and uploads to the platform.

4. What Personal Information We Collect

4.1 Information You Provide Directly

Category	Examples
Account information	Name, email address, password (stored as a cryptographic hash), role, organisation membership
Client organisation data	Organisation name, type, data region preference
Application and project data	Project names, descriptions, assessment criteria and scores, supporting documents, budget information, narrative responses
Program and cohort data	Program names, descriptions, cohort structures, intake periods
Uploaded documents	Any files uploaded to the platform by clients or applicants, which may contain Personal Information, Sensitive Information, financial data, or proprietary content
Communications	Emails, support requests, feedback, task notes, in-platform comments

4.2 Information We Collect Automatically

Category	Examples
Log data	IP address, browser type and version, operating system, referring URL, pages visited, date and time of access
Cookies	Session cookies for authentication, CSRF security tokens (see Section 11)
Usage data	Features accessed, reports generated and downloaded, actions taken within the portal, frequency and duration of use
Consent records	Records of consents granted or revoked, including timestamps and IP addresses

4.3 Information We Receive From Third Parties

We may receive Personal Information about you from:

- Your employer or organisation administrator, who creates or manages your account or invites you to the platform
- Invitation links shared by existing users

4.4 Sensitive Information and Special Category Data

We do not intentionally collect Sensitive Information unless it is voluntarily included by applicants or clients in uploaded documents, application forms, or free-text fields. Examples may include information about disability status, cultural background, health conditions, or personal circumstances disclosed in project applications.

Where Sensitive Information is provided:

- We rely on the client (as Data Controller) to have obtained appropriate consent or to have established another lawful basis for its collection
- We treat it with the highest level of care and restrict access to authorised personnel only
- We do not use Sensitive Information for any purpose other than providing the services requested by the client
- Under GDPR, processing of special category data is limited to the bases set out in Article 9(2)

5. How We Use Your Personal Information

Purpose	Description	Legal Basis (GDPR)
Providing our services	Operating the platform, processing applications, managing projects and cohorts, generating reports, hosting uploaded documents	Performance of a contract / Legitimate interest
Authentication and security	Verifying identity, managing sessions, preventing unauthorised access, recording consent	Performance of a contract / Legitimate interest
Data analysis and reporting	Running our proprietary assessment algorithms and AI-powered analysis (including LLM-based processing via Amazon Bedrock) on submitted application data to produce analytical reports (see Section 6)	Performance of a contract
Administration	Managing client relationships, invitations, user roles, and billing	Performance of a contract
Communication	Responding to enquiries, providing support, sending service-related notifications	Legitimate interest
Platform improvement	Analysing usage patterns to improve features, fix bugs, and develop new functionality	Legitimate interest
Aggregated insights	Producing de-identified, aggregated statistical insights across the platform (see Section 6.5)	Legitimate interest
Legal compliance	Complying with applicable laws, regulations, and legal processes	Legal obligation

We will not use your Personal Information for purposes materially different from those described above without first notifying you and, where required, obtaining your consent. We will never sell Personal Information to third parties. We will not use Client Data for marketing purposes.

6. Data Science, Automated Processing, and Algorithmic Analysis

6.1 What We Do

Adoptic uses proprietary data science methodologies, algorithms, and AI-powered analysis to analyse application data submitted by clients. This includes:

- Scoring and assessment — calculating Desirability, Adoptability, Feasibility, Viability, and Psychosocial scores based on structured application data
- AI-powered analysis — submitting application text to large language models (LLMs) via Amazon Bedrock for quote extraction, argument generation, evidence verification, and scoring as part of a multi-step analytical pipeline (see Section 6.7)
- Statistical analysis — producing descriptive statistics, distributions, benchmarks, and comparative analyses across cohorts and programs
- Report generation — compiling analytical outputs into structured reports (Audit Reports, Assessor's Aids, Cohort Reports, Comparison Reports, Guidance Reports)
- Data visualisation — generating charts, graphs, and visual representations of analytical findings

6.2 Automated Decision-Making and Profiling

Our algorithms produce analytical outputs (scores, rankings, and statistical summaries) that are designed to inform and support human decision-making by our clients. Specifically:

- No solely automated decisions: Adoptic does not make decisions that produce legal effects or similarly significant effects on individuals based solely on automated processing. Although our analytical pipeline includes AI/LLM processing (see Section 6.7), LLM outputs are intermediate inputs — they are structured, validated, and combined with other analytical steps before producing final scores. Our outputs are advisory tools intended to assist client decision-makers, not replace them.
- Human oversight: All final decisions about applications, funding, or other outcomes remain with the client organisation's authorised personnel. Adoptic's role is to provide data-driven analysis, not to determine outcomes. No individual outcome is determined solely by an AI model.
- Transparency of methodology: Our analytical methodologies are documented and can be explained to clients upon request. We do not operate opaque "black box" algorithms. Clients receive documentation describing the rationale, inputs, weightings, and limitations of our scoring models.
- No profiling for marketing: We do not use Personal Information to build profiles for targeted advertising, credit scoring, or any purpose unrelated to the services contracted

by the client.

6.3 Rights Relating to Automated Processing

Under Article 22 of the UK/EU GDPR, individuals have the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. Because Adoptic's outputs are advisory and require human review before any consequential decision is made, Article 22 does not apply to our standard processing. However, if you believe an automated output has been used to make a decision about you without adequate human involvement, you may:

- Request an explanation of the logic involved in the processing
- Request human review of the output
- Express your point of view and contest the decision

These requests should be directed to the client organisation that administers your data. If the client is unable to assist, you may contact Adoptic directly.

6.4 Derived Data and Intellectual Property

- Client Data ownership: Clients retain ownership of all data they upload to or create within the platform (Client Data). Adoptic does not claim ownership of Client Data.
- Derived Data: Analytical outputs (scores, reports, statistical summaries) generated by Adoptic's algorithms from Client Data are produced for the exclusive benefit of the client and are treated as confidential to that client.
- Proprietary algorithms: The algorithms, methodologies, models, and software used to produce Derived Data are the intellectual property of Adoptic. Clients receive the outputs but do not acquire rights to the underlying algorithms or source code.
- No cross-client use: We do not use one client's identifiable data to produce outputs for another client.

6.5 Aggregated and De-identified Data

We may produce aggregated, de-identified data drawn from across the platform to:

- Improve our algorithms and analytical methodologies
- Produce sector-wide benchmarks and statistical insights
- Publish anonymised sample reports for demonstration purposes

This aggregated data is stripped of all identifiers and cannot reasonably be used to identify any individual or client organisation. Where we use Client Data for these purposes, we apply robust de-identification techniques and will not attempt to re-identify individuals from aggregated data.

6.6 Model Training and Improvement

Where we use data to develop, train, or improve our analytical models:

- We use only de-identified and aggregated data, not identifiable Client Data
- We do not use Client Data to train models for unrelated purposes
- Clients may opt out of having their de-identified data included in aggregated datasets used for model improvement by notifying us in writing

6.7 AI and Large Language Model Processing

Adoptic's analytical pipeline includes processing of Client Data using large language models (LLMs) provided through Amazon Bedrock, a managed AI service operated by Amazon Web Services (AWS). This section describes how that processing works and the safeguards in place.

What data is sent to the LLM:

- Full application text submitted by applicants (narrative responses, project descriptions, supporting information)
- Assessment variable definitions and scoring criteria defined by the client
- Not sent: User credentials, account information, billing data, or raw uploaded files (only extracted text content relevant to the assessment)

How data is processed:

- Application text is submitted to the LLM (Claude, developed by Anthropic, hosted on Amazon Bedrock) as part of a four-step analytical pipeline: (1) quote extraction, (2) argument generation, (3) evidence verification, and (4) scoring
- Approximately 70 LLM calls are made per application, covering each assessment variable across the pipeline steps
- LLM outputs are structured scores, extracted quotes, and analytical reasoning — these are intermediate inputs that feed into Adoptic's broader scoring and reporting engine
- Each LLM invocation is independent; no data from one client's application is used in the processing of another's

Where data is processed:

- All LLM processing occurs in the ap-southeast-2 (Sydney, Australia) AWS region
- No Client Data is transferred overseas for LLM processing

Data retention by the LLM provider:

- Amazon Bedrock does not retain, store, or log input or output data for model training or improvement
- Input and output data is not shared with model providers (Anthropic) or across AWS customers

- Data is encrypted in transit (TLS) and at rest by AWS
- Ephemeral prompt caching may be used for system prompts within a session; cached content is not persisted and is not accessible to other customers

No use of Client Data for AI training:

- Client Data is never used to fine-tune, train, or improve any AI or machine learning model, whether by Adoptic, AWS, or Anthropic
- This is a contractual guarantee provided by Amazon Bedrock's terms of service

Security and compliance:

- Amazon Bedrock is SOC 2 Type II and ISO/IEC 27001 certified
- Access to Bedrock is authenticated via AWS IAM credentials managed by Adoptic
- Processing is confined to the ap-southeast-2 region and subject to Australian data residency

7. Disclosure of Personal Information

7.1 Your Organisation

If you are a user within a client organisation, your organisation's administrators may have access to your account details, activity within the platform, and data you submit. The extent of access is determined by the organisation's role-based settings.

7.2 Service Providers (Sub-processors)

We use trusted third-party service providers to operate and support our platform. These providers are contractually required to protect your information and may only use it to perform services on our behalf. They are subject to obligations no less protective than those in this policy.

Provider	Purpose	Data Location
Amazon Web Services (AWS)	Cloud hosting, data storage, infrastructure, backups	[REGION]
Amazon Bedrock (AWS)	AI-powered application analysis using large language models (see Section 6.7)	ap-southeast-2 (Sydney)
Railway	Application hosting (transitioning to AWS)	United States
[EMAIL PROVIDER]	Transactional email delivery	[REGION]

Provider	Purpose	Data Location
[PAYMENT PROVIDER]	Payment processing (if applicable)	[REGION]

We maintain a current list of sub-processors and will update this section when sub-processors are added or changed. Clients under Data Processing Agreements will be notified of sub-processor changes in advance.

7.3 Legal and Regulatory

We may disclose Personal Information where required or authorised by law, including:

- To comply with a legal obligation, subpoena, warrant, or court order
- To enforce our terms of use or protect our rights, property, or safety
- To protect the safety of any person
- To investigate suspected fraud, security incidents, or violations of our terms
- To government agencies or regulatory bodies as required by applicable law

7.4 Business Transfers

In the event of a merger, acquisition, restructure, or sale of all or part of our business, Personal Information may be transferred to the successor entity, subject to this Privacy Policy. We will notify affected users and clients before any such transfer and provide an opportunity to request deletion of data.

7.5 De-identified and Aggregated Data

We may share de-identified or aggregated data that cannot reasonably be used to identify any individual. For example, we publish anonymised sample reports on our website for demonstration purposes. See Section 6.5 for details.

7.6 With Your Consent

We may disclose Personal Information to other parties where you have given explicit consent.

8. Overseas Disclosure and International Transfers

Some of our service providers are located outside Australia. As at the date of this policy, Personal Information may be transferred to or stored in:

- United States — Railway hosting, [other providers]

- [Other regions as applicable]

Note: AI/LLM processing via Amazon Bedrock is performed entirely within the ap-southeast-2 (Sydney, Australia) region. No Client Data is transferred overseas for AI processing.

Before disclosing Personal Information overseas, we take reasonable steps to ensure that the recipient handles it in accordance with the APPs and does not breach the Australian Privacy Principles (APP 8).

Where UK/EU GDPR applies, international transfers are made only where:

- The destination country has been granted an adequacy decision by the European Commission or UK government, or
- Appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs), or
- A derogation under Article 49 of the GDPR applies

Details of the safeguards relied upon for specific transfers are available on request.

9. Data Security

We take reasonable steps to protect Personal Information from misuse, interference, loss, and unauthorised access, modification, or disclosure. Our security measures include:

- Encryption in transit — all data transmitted between your browser and our servers is encrypted using TLS 1.2+ (HTTPS)
- Encryption at rest — data stored on our servers is encrypted using industry-standard encryption (AES-256)
- Password hashing — user passwords are stored using PBKDF2-SHA256 cryptographic hashing and are never stored or logged in plain text
- Access controls — role-based access ensures users only see data relevant to their role and organisation
- Organisation-level data isolation — client data is logically separated and enforced at the application layer
- Invite-only access — new accounts are created via secure, time-limited invitation links
- Audit logging — significant actions within the platform are logged for accountability

For further detail, refer to our separate Data Security Policy.

10. Data Retention

We retain Personal Information for as long as necessary to fulfil the purposes described in this policy, or as required by law. Specifically:

Data Type	Retention Period
User accounts	Duration of the account plus [X] years after deletion or deactivation
Client Data	Duration of the client contract plus [X] years, unless the client requests earlier deletion
Derived Data (reports, scores)	Same as the Client Data from which it was derived
Log and usage data	[X] months from collection
Consent records	[X] years after revocation or account deletion
Aggregated / de-identified data	Retained indefinitely (not Personal Information)

When Personal Information is no longer required, we will take reasonable steps to destroy or de-identify it.

10.1 Client-Initiated Deletion

Clients may request deletion of their Client Data at any time. Upon receiving a verified deletion request:

- We will delete or de-identify all Client Data within [X] business days
- We will confirm deletion in writing
- Backups containing the data will be overwritten in the normal rotation cycle (typically within [X] days)
- Aggregated, de-identified data derived prior to deletion may be retained

10.2 Data Portability and Export

Clients may request an export of their Client Data in a structured, commonly used, machine-readable format (e.g., CSV, JSON, PDF). We will fulfil such requests within [X] business days. This right also applies to individuals under GDPR Article 20 where processing is based on consent or contract and carried out by automated means.

11. Cookies

We use cookies to operate the platform:

Cookie	Type	Purpose	Duration
Session cookie	Strictly necessary	Maintains your authenticated session	Browser close or [X] hours of inactivity
CSRF token	Strictly necessary	Prevents cross-site request forgery	Session

We do not use:

- Advertising or retargeting cookies
- Third-party tracking or analytics cookies
- Social media cookies

You can control cookies through your browser settings. However, disabling strictly necessary cookies will prevent you from using the authenticated features of the platform.

12. Your Rights

12.1 Under the Australian Privacy Act

You have the right to:

- Access the Personal Information we hold about you (APP 12)
- Request correction of inaccurate, out-of-date, incomplete, irrelevant, or misleading information (APP 13)
- Complain about a breach of the Australian Privacy Principles
- Anonymity / pseudonymity — where practicable, you have the option of not identifying yourself or using a pseudonym (APP 2). This may not be practicable for authenticated features.

12.2 Under UK/EU GDPR (where applicable)

If you are located in the UK or EEA, you also have the right to:

- Erasure ("right to be forgotten") — request deletion of your Personal Information (Article 17)
- Restriction — request that we limit processing in certain circumstances (Article 18)
- Portability — receive your data in a structured, machine-readable format (Article 20)
- Objection — object to processing based on legitimate interest (Article 21)
- Withdraw consent — where processing is based on consent, withdraw at any time (Article 7)

- Automated decision-making — not be subject to solely automated decisions with significant effects; request human intervention (Article 22; see also Section 6.3)

12.3 How to Exercise Your Rights

To make a request, contact us at [PRIVACY CONTACT EMAIL]. We will:

- Acknowledge your request within 5 business days
- Respond substantively within 30 days (or the timeframe required by applicable law)
- Verify your identity before processing your request
- Not charge a fee for reasonable requests

Where we act as a Data Processor and receive a request from an individual, we will refer the request to the relevant client (Data Controller) unless directly required by law to respond.

13. Client Responsibilities

Adoptic operates as a Data Processor on behalf of our clients (the Data Controllers). Our clients are responsible for:

- Ensuring they have appropriate lawful bases to collect and process Personal Information through the platform
- Providing clear and comprehensive privacy notices to their applicants, assessors, and stakeholders
- Obtaining any necessary consents before uploading Personal Information (including Sensitive Information) to the platform
- Responding to data subject access requests and other rights requests from individuals whose data they control
- Complying with applicable privacy and data protection laws in their jurisdiction
- Notifying Adoptic if they become aware of any data breach affecting data held on the platform

13.1 Data Processing Agreements

We enter into Data Processing Agreements (DPAs) with clients to formalise the terms on which we process Personal Information on their behalf. DPAs address:

- The subject matter, duration, nature, and purpose of processing
- The types of Personal Information and categories of data subjects
- The obligations and rights of the Data Controller
- Sub-processor arrangements and notification obligations

- Security measures and audit rights
- Data breach notification procedures
- Data return and deletion on termination

Clients requiring a DPA should contact [PRIVACY CONTACT EMAIL].

14. Document Uploads and Client-Controlled Content

Clients and their users may upload documents and files to the platform. Adoptic:

- Stores uploaded documents securely using the infrastructure described in our Data Security Policy
- Does not review, screen, or moderate the content of uploaded documents unless required for technical support or legal compliance
- Does not claim any ownership of or licence to uploaded documents beyond what is necessary to store, display, and process them as part of the service
- Treats all uploaded documents as Confidential Client Data
- Restricts access to uploaded documents to authorised users within the relevant client organisation and authorised Adoptic personnel

Clients are responsible for ensuring that they have the right to upload any documents and that such documents comply with applicable laws. Clients must not upload content that is unlawful, infringes third-party rights, or contains malicious code.

15. Complaints

If you believe we have breached the Australian Privacy Principles or your rights under applicable law, you may lodge a complaint with us. We will acknowledge your complaint within 5 business days, investigate the matter, and respond within 30 days.

If you are not satisfied with our response, you may escalate your complaint to:

Office of the Australian Information Commissioner (OAIC)

Website: www.oaic.gov.au · Phone: 1300 363 992

Information Commissioner’s Office (ICO) (for UK/EEA residents)

Website: www.ico.org.uk · Phone: 0303 123 1113

16. Children’s Information

Adoptic does not knowingly collect Personal Information from children under the age of 16. Our platform is designed for use by organisations and their authorised personnel, not by children directly. If we become aware that we have collected Personal Information from a child without appropriate consent, we will take steps to delete it promptly.

17. Changes to This Policy

We may update this Privacy Policy from time to time. When we make changes:

- We will post the updated policy on our website with a revised version date
- Material changes will be communicated to registered users by email or through the platform at least 14 days before they take effect
- Continued use of the platform after changes take effect constitutes acceptance of the updated policy

18. Related Policies

This Privacy Policy should be read together with:

- Data Security Policy — technical and organisational measures for protecting data
- Terms of Use — conditions of access to the platform
- Cookies Declaration — detailed information about cookies used
- Third-Party Service Providers — current list of sub-processors

19. Contact Us

[ADOPTIC PTY LTD]

ABN: [XX XXX XXX XXX]

Address: [REGISTERED ADDRESS]

Email: [PRIVACY CONTACT EMAIL]

Website: adoptic.online

This policy was last updated on [DATE].