

DEXIFY AI PTY LTD

PRIVACY POLICY

Contracting entity: Dexify AI Pty Ltd ACN 698 912 882, trading as Dexify AI

Website: dexifyai.com

Effective date: 01/08/2026

Version: 1.0

Status: Website publication copy

Introduction

This Privacy Policy (Policy) explains how Dexify AI Pty Ltd ACN 698 912 882, trading as Dexify AI (Dexify, we, us or our), collects, holds, uses, discloses, stores and otherwise handles personal information when you access or use our AI-powered administration platform, website, mobile application, application programming interfaces and related products, features, support and services (the Service).

This Policy is prepared in accordance with the Privacy Act 1988 (Cth) (Privacy Act) and the Australian Privacy Principles (APPs). Where you are located outside Australia, we also endeavour to comply with applicable privacy laws in your jurisdiction, including the General Data Protection Regulation (EU/UK GDPR), the California Consumer Privacy Act (CCPA) and equivalent frameworks, to the extent they apply to our processing of your personal information.

This Policy forms part of, and should be read together with, our Terms of Service. Capitalised terms used but not defined in this Policy have the meaning given to them in the Terms of Service.

By creating an Account, using the Service or otherwise providing personal information to us, you acknowledge that you have read and understood this Policy. If you do not agree with this Policy, you must not access or use the Service.

1. Definitions and interpretation

1.1 Definitions

In this Policy:

- **Account** means an account registered to access the Service.
- **Account Owner** means the person or entity identified as the owner or administrator of an Account.
- **APPs** means the Australian Privacy Principles set out in Schedule 1 of the Privacy Act.
- **Authorised User** means an employee, contractor or other individual whom the Customer authorises to use the Service under its Account.
- **Customer** means the person or entity that creates an Account, purchases a Subscription or otherwise accesses or uses the Service.
- **Customer Data** means data, content, recordings, documents, materials and information submitted to, stored in, transmitted through or generated from the Customer's use of the Service, excluding Dexify

Materials and de-identified or aggregated data that cannot reasonably identify the Customer or an individual.

- **NDB Scheme** means the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act.
- **Output** means content generated by or through the Service in response to Customer Data or instructions.
- **Partner** means an approved affiliate or eligible Customer participating in our Affiliate and Referral Program.
- **Personal Information** has the meaning given in the Privacy Act and, where the GDPR applies, includes personal data as defined in the GDPR.
- **Privacy Act** means the Privacy Act 1988 (Cth).
- **Sensitive Information** has the meaning given in section 6 of the Privacy Act and, where the GDPR applies, includes special categories of data as defined in the GDPR.
- **Service** means the Dexify products and services as described above.
- **Subprocessor** means a third-party service provider engaged by Dexify to process Personal Information on its behalf.
- **Third-Party Service** means a service, platform, software, model, infrastructure provider or integration supplied by a third party.
- **Website** means dexifyai.com and any replacement or related website operated by us.

1.2 Interpretation

Headings are for convenience only. The words including, for example and similar expressions do not limit the words that precede them. The singular includes the plural and vice versa. A reference to a law includes amendments and replacements.

2. Information we collect

We collect and process Personal Information that is reasonably necessary for, or directly related to, the functions and activities of the Service. We collect information in the following categories.

2.1 Account and identity information

When you create an Account or purchase a Subscription, we collect:

- full name and business name;
- email address and phone number;
- business identifier number (such as ABN, GST registration number, VAT number or equivalent in your jurisdiction);
- business address, service area and trade type;
- business profile details, logo and branding materials you upload; and
- password or third-party authentication credentials (we store passwords in hashed form only and do not store complete credentials from third-party sign-in services).

2.2 Voice and audio data

Where you use the voice assistant feature, we collect:

- voice recordings and audio files you record, upload or transmit through the Service;

- transcripts generated from voice recordings;
- extracted intent, commands, entities and structured data derived from voice processing; and
- text-to-speech outputs delivered back to you.

2.3 Business and client data

When you use the Service to create quotes, invoices, job records, schedules and other documents, you may input data about your clients, staff and business operations, including:

- client contact details (name, address, phone number, email);
- job-specific information, site details and scope of work;
- material, labour and pricing data;
- scheduling and calendar information; and
- notes, photos and attachments relating to jobs.

You are responsible for ensuring you have appropriate authorisation, consent and a lawful basis to submit any third-party information into the Service.

2.4 Usage and interaction data

We automatically collect information about how you interact with the Service, including:

- queries, commands and interactions with the AI system;
- features accessed, pages viewed and actions taken;
- session duration, frequency of use and workflow patterns;
- app usage logs and feature interaction data; and
- error reports, crash logs and diagnostic data.

2.5 Technical and device information

We automatically collect certain technical information, including:

- IP address and approximate geolocation derived from it;
- device type, model, operating system and version;
- browser type and version;
- unique device identifiers and mobile advertising identifiers;
- referral URLs and landing pages; and
- network connection type.

2.6 Payment and billing information

When you purchase a Subscription, payment processing is handled by our third-party payment provider. We do not store complete credit card or debit card numbers. We may receive and store:

- billing name and address;
- last four digits of payment card number and card type;
- payment transaction identifiers and status; and
- invoice and billing history.

2.7 Affiliate and referral partner information

If you participate in our Affiliate and Referral Program, we additionally collect:

- your name and the name of your business or organisation;
- email address and contact details;
- unique referral link or code and associated tracking data;
- bank account details (including BSB, account number and account holder name) and any other payment information necessary to distribute commissions and referral earnings to you;
- social media handles or public profile details relevant to your participation; and
- tax information such as ABN, tax file declaration or equivalent, where required for payment.

2.8 Communications and support data

When you contact us for support or communicate with us, we collect:

- the content of emails, chat messages and support tickets;
- feedback, suggestions and survey responses; and
- call recordings where disclosed at the time of the call.

2.9 Information from third-party sources

We may receive Personal Information from third-party sources, including:

- third-party sign-in services (such as Google or Apple) if you choose to register or log in using those services;
- publicly available business information, such as ABN and registration details; and
- analytics and attribution data from advertising or referral partners.

2.10 Sensitive information

We do not intentionally collect Sensitive Information (such as health information, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal record or biometric data). If Sensitive Information is inadvertently included in voice recordings, transcripts or other Customer Data, we will treat it in accordance with the heightened protections required by law. You should avoid recording or uploading Sensitive Information unless it is necessary, lawful and appropriate for your use of the Service.

3. How we collect personal information

3.1 Direct collection

We collect most Personal Information directly from you when you create an Account, use the Service, contact us for support, participate in the Affiliate Program, complete forms or surveys, or otherwise provide information to us.

3.2 Automatic collection

We automatically collect technical, device, usage and interaction data through the Service, cookies and similar technologies as described in clause 9.

3.3 Collection from third parties

We may collect Personal Information from third parties as described in clause 2.9. Where we do so, we will handle it in accordance with this Policy and applicable law.

3.4 Anonymity and pseudonymity

Where it is lawful and practicable, you may deal with us on an anonymous or pseudonymous basis. However, if you do not provide certain information, we may not be able to provide the Service or respond to your enquiry.

4. Purposes for which we collect, hold, use and disclose personal information

We collect, hold, use and disclose Personal Information for the following purposes:

4.1 Service delivery and operation

- providing, operating, maintaining and improving the Service;
- processing voice input and generating Outputs including quotes, invoices, job notes and schedules;
- personalising your experience using your business data and preferences;
- managing your Account, Subscription and billing;
- providing customer support and responding to enquiries; and
- enabling integrations with Third-Party Services you connect.

4.2 AI processing and Outputs

The Service uses automated and artificial intelligence systems to process your data and generate Outputs. This includes transmitting your data, including voice input, customer details, job information and other content, to third-party large-language-model providers such as OpenAI, Anthropic (Claude) and Google (Gemini), and voice processing providers such as Deepgram. Further detail is provided in clause 7.

4.3 Security and integrity

- detecting, preventing and investigating fraud, misuse, security incidents and unlawful activity;
- enforcing our Terms of Service and other agreements;
- maintaining the security, stability and integrity of the Service; and
- conducting security audits and vulnerability assessments.

4.4 Analytics and improvement

- analysing usage patterns, trends and performance metrics to improve the Service;
- conducting internal research and development;
- benchmarking and quality assurance; and
- developing new features, products and services.

Product analytics or service improvement using identifiable Customer Data is permitted only to the extent described in this Policy and reasonably necessary for those purposes.

4.5 Communications

- sending operational, security, billing, legal and account communications;
- providing product updates, feature announcements and service notices;
- sending marketing communications where you have consented or where permitted by law; and
- conducting surveys and collecting feedback.

4.6 Legal and regulatory compliance

- complying with applicable laws, regulations, codes of practice and lawful requests;
- responding to subpoenas, court orders and legal process;
- establishing, exercising or defending legal claims; and
- meeting record-keeping, tax and audit obligations.

4.7 Affiliate and referral program administration

- tracking referrals and attributing sign-ups to Partners;
- calculating, approving and processing commissions and payouts;
- administering Partner accounts and compliance; and
- preventing fraud, duplicate accounts and program abuse.

5. Disclosure of personal information

We do not sell your Personal Information. We may disclose Personal Information to the following categories of recipients for the purposes described in this Policy:

5.1 Service providers and subprocessors

We engage trusted third-party service providers (Subprocessors) to operate our infrastructure and deliver the Service. These providers are bound by contractual confidentiality obligations and may only process data as directed by us and for the purposes specified. Our current categories of Subprocessors include:

- cloud infrastructure and hosting (Google Cloud Platform);
- database services (Google Cloud SQL);
- voice processing and transcription (Deepgram);
- AI and large-language-model providers (OpenAI, Anthropic, Google);
- transactional email delivery (SendGrid);
- payment processing (Stripe or other disclosed provider);
- analytics and monitoring services;
- referral tracking and affiliate payout services; and
- customer support and communication tools.

A current Subprocessor List identifying the specific providers that process Customer Data on our behalf is maintained and made available upon request. We will give reasonable notice of material changes to our Subprocessor List.

5.2 AI and large-language-model providers

To provide the Service, we transmit your data, including voice input, customer details, job information and other content you supply, to third-party large-language-model providers such as OpenAI, Anthropic (Claude) and Google (Gemini). We select providers and configure integrations using commercially reasonable security measures. Once data is transmitted, it is also subject to that provider's own terms, privacy policy and data-handling practices. We may change, add or remove providers at any time without prior notice.

By using the Service, you acknowledge and consent to this transmission. You should not input data through the Service that you are not permitted to share with a third-party cloud provider, and you remain responsible for obtaining any consents required from your customers or other individuals whose Personal Information you submit.

5.3 Affiliate and referral program disclosures

Partners can see whether a referral they generated has converted into a paying customer and the commission earned. Partners do not have access to the referred customer's Personal Information, business data, pricing or job records.

5.4 Professional advisers

We may disclose Personal Information to our legal, accounting, insurance and other professional advisers in connection with obtaining advice, managing claims or conducting audits.

5.5 Related bodies corporate

We may disclose Personal Information to our related bodies corporate (as defined in the Corporations Act 2001 (Cth)) for the purposes described in this Policy.

5.6 Corporate transactions

In connection with a merger, acquisition, restructure, sale of assets or business, financing or similar transaction, Personal Information may be disclosed to prospective parties and their advisers, subject to confidentiality obligations. If such a transaction proceeds, the successor entity will be bound by this Policy with respect to the Personal Information transferred.

5.7 Legal requirements and safety

We may disclose Personal Information where required or permitted by law, court order, subpoena, regulatory authority or government agency, or where we reasonably believe disclosure is necessary to:

- comply with applicable law, regulation or legal process;
- protect the rights, property, safety or security of Dexify, our users or the public;
- detect, prevent or investigate fraud, security incidents or unlawful activity;
- enforce our Terms of Service or other agreements; or
- respond to an emergency involving danger to any person.

6. Cross-border disclosure of personal information

6.1 Countries of disclosure

As a platform that uses global infrastructure and service providers, your Personal Information may be stored, processed or disclosed in countries other than Australia, including the United States of America, and any other country where our Subprocessors maintain infrastructure.

6.2 Safeguards

Before disclosing Personal Information to an overseas recipient, we take reasonable steps to ensure that the recipient does not breach the APPs (or, where the GDPR applies, that an adequate level of protection is ensured through appropriate safeguards such as standard contractual clauses, adequacy decisions or binding corporate rules). However, by using the Service, you acknowledge that overseas recipients may not be subject to privacy obligations equivalent to the APPs or other Australian privacy laws, and the protections available under those laws may not be available in the recipient's jurisdiction.

6.3 Consent to overseas disclosure

Where required by APP 8.2(b), by using the Service and agreeing to this Policy, you consent to the disclosure of your Personal Information to overseas recipients in the circumstances described above. This consent means that we will not be accountable under the Privacy Act for acts or practices of the overseas recipient that would breach the APPs, except to the extent required by law.

7. AI processing, automated decision-making and model training

7.1 AI-assisted features

The Service uses automated and artificial intelligence systems to process your data and generate Outputs, including draft quotes, invoices, job notes, schedules, descriptions, summaries and transcripts. These Outputs may be incomplete, inaccurate, non-unique, unsuitable, outdated or misleading. You must review and independently verify all Outputs before relying on, sending, publishing or acting on them. Outputs are not professional advice.

7.2 Automated decision-making

The Service does not make legally binding or significant decisions about individuals solely through automated processing. AI-generated content is provided as a draft or suggestion for your review and approval. You retain full responsibility for the accuracy and legal effect of documents you issue.

7.3 No use of Customer Data for model training

We will not use identifiable Customer Data to train or fine-tune any generative AI model, whether general-purpose or Dexify-specific, unless the Customer expressly opts in after clear disclosure of the nature and purpose of such use.

7.4 Human review

We may conduct limited human review of Customer Data only where reasonably necessary for requested support, security, abuse investigation, legal compliance or quality assurance described in this Policy, and only by authorised personnel subject to confidentiality obligations.

7.5 De-identified and aggregated data

We may use properly de-identified or aggregated information that cannot reasonably identify you, your clients or another individual for analytics, security, benchmarking, service improvement and model or system evaluation. De-identification is performed using techniques designed to prevent re-identification, in accordance with applicable law and industry standards.

8. Voice data

8.1 Voice processing

Voice recordings are processed to generate transcripts, extract intent, commands and structured data. Text-to-speech technology is used to deliver AI-generated responses back to you. Voice processing is currently powered by Deepgram and may involve other disclosed providers.

8.2 Use of voice data

Voice recordings and derived data are:

- used solely to power the voice assistant functionality and provide the Service;
- transmitted to third-party voice processing and AI providers as described in clause 5.2;

- not used to train third-party AI models without your explicit consent; and
- stored for the period described in clause 11 and then deleted or de-identified.

8.3 Your obligations

Before recording, uploading or processing a conversation, voice message or audio file, you must ensure that you are legally permitted to do so, provide any notices required by law and obtain all required consents. Recording and surveillance laws differ between Australian jurisdictions and in other countries. You must not use the Service for covert or unlawful surveillance, interception or recording.

8.4 Voice data deletion

You may request deletion of your voice data at any time by contacting us at contact@dexifyai.com.

9. Cookies and tracking technologies

9.1 What we use

We use cookies and similar technologies (such as local storage, pixels and web beacons) to:

- maintain session state and authenticate users;
- remember your preferences and settings;
- analyse usage patterns and improve the Service;
- measure the effectiveness of communications; and
- attribute referral sign-ups for our Affiliate and Referral Program.

9.2 Affiliate tracking cookies

If you sign up through an Affiliate or Referral Partner's link or code, we set a tracking cookie to attribute your sign-up to that Partner. This cookie currently lasts for 100 days and does not collect any Personal Information beyond the referral attribution itself. It is used solely to administer Partner commissions and not to track you for advertising or analytics purposes elsewhere.

9.3 Third-party cookies

We do not use cookies to serve third-party advertising, and we do not sell data to advertising networks. Third-party service providers integrated into the Service may set their own cookies subject to their privacy policies.

9.4 Managing cookies

You can control cookie settings through your browser or device settings. Disabling cookies may affect certain features of the Service, including session management and a Partner's ability to be credited for a referral. Where required by applicable law, we will obtain your consent before setting non-essential cookies.

10. Data security

10.1 Security measures

We implement reasonable technical and organisational safeguards appropriate to the nature of the Service and the Personal Information processed. These measures include, but are not limited to:

- encryption of data in transit using TLS/SSL;

- encryption of sensitive data at rest;
- access controls, role-based permissions and principle of least privilege;
- secure credential management and multi-factor authentication;
- regular security reviews, vulnerability assessments and monitoring;
- incident response procedures and business continuity planning; and
- confidentiality obligations for personnel and subcontractors who access Personal Information.

10.2 No guarantee

No internet service is completely secure. We do not guarantee that unauthorised access, loss, destruction, use, modification or disclosure of Personal Information will never occur. You acknowledge that the transmission of information over the internet carries inherent risks.

10.3 Customer security obligations

You must secure your devices, networks, accounts and integrations; use appropriate access controls and authentication; maintain current software; keep credentials and authentication methods confidential; and promptly notify us at contact@dexifyai.com of suspected unauthorised access, credential compromise or security issues affecting the Service or Customer Data.

11. Data retention and deletion

11.1 Retention periods

We retain Personal Information for as long as reasonably necessary to fulfil the purposes for which it was collected, comply with legal obligations and resolve disputes. Our standard retention periods are:

- Account and business data: retained for the duration of your Subscription and up to 7 years after account closure, in line with Australian tax and business record-keeping requirements.
- Voice recordings: retained for the period necessary to provide the voice assistant functionality, unless you request earlier deletion.
- Transcripts and Outputs: retained for the duration of your Subscription and the post-termination export period.
- Usage logs and analytics: retained for up to 12 months.
- Support correspondence: retained for up to 3 years.
- Payment and billing records: retained for up to 7 years for tax and audit purposes.
- Affiliate and Referral Program records (Partner details, referral tracking, commission and payout history): retained for the duration of the Partner's participation and up to 7 years afterwards, in line with Australian tax record-keeping requirements.
- **Lifetime Subscription data:** for Customers whose accounts are terminated due to cessation of the Service, data will be retained for 90 days following termination to allow for data export, after which it will be deleted in accordance with this Policy.

11.2 Post-termination access

For an ordinary cancellation, we will use reasonable efforts to make available a data-export opportunity for at least 30 days after access ends, unless law, security, non-payment, serious misuse or technical limitations require a shorter period. You should export data before cancellation or downgrade.

11.3 Deletion and de-identification

After the applicable retention period, we may delete or de-identify Personal Information. Information may remain temporarily in backups, logs and disaster-recovery systems and may be retained where reasonably necessary for legal, tax, accounting, fraud-prevention, security, dispute or enforcement purposes.

11.4 Data deletion requests

You may request deletion of your Personal Information at any time (see clause 12). Deletion is subject to applicable legal retention requirements and technical limitations.

12. Your rights

12.1 Rights under the Privacy Act

Under the Privacy Act and APPs, 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 Personal Information (APP 13); and
- complain about how we have handled your Personal Information (APP 1).

12.2 Additional rights under the GDPR

Where the GDPR applies to our processing of your Personal Information, you may also have the right to:

- request erasure of your Personal Information (right to be forgotten);
- restrict processing of your Personal Information;
- object to processing based on legitimate interests or direct marketing;
- data portability (receive your data in a structured, commonly used, machine-readable format);
- withdraw consent at any time where processing is based on consent; and
- not be subject to a decision based solely on automated processing that produces legal or similarly significant effects.

12.3 Additional rights under the CCPA

Where the CCPA applies, California residents may also have the right to:

- know the categories and specific pieces of Personal Information collected;
- request deletion of Personal Information;
- opt out of the sale or sharing of Personal Information (we do not sell Personal Information); and
- not be discriminated against for exercising privacy rights.

12.4 How to exercise your rights

To exercise any of these rights, send an email to contact@dexifyai.com with the subject line 'Privacy Request' and include your full name and the email address associated with your Dexify Account. We may require reasonable identity verification before processing your request. We will respond within 30 days (or such shorter period as required by applicable law).

12.5 Complaints

If you are not satisfied with our response to a privacy complaint, you may lodge a complaint with:

- the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au (for Australian privacy law matters);
- the relevant data protection authority in your jurisdiction (for GDPR or other international privacy law matters); or
- any other applicable regulatory body.

13. Children's privacy

The Service is not intended for use by individuals under the age of 18. We do not knowingly collect Personal Information from children. If you believe we have inadvertently collected Personal Information from a minor, please contact us immediately at contact@dexifyai.com and we will take steps to delete it.

14. Direct marketing

14.1 Marketing communications

We may use your email address and other contact details to send you marketing communications about our products, services, features, promotions and events, where you have consented or where permitted by applicable law (including under the Spam Act 2003 (Cth)).

14.2 Opt-out

You may opt out of marketing communications at any time by using the unsubscribe link in the communication or by contacting us at contact@dexifyai.com. Opting out of marketing does not affect essential service, billing and account communications.

14.3 No sale of data for marketing

We do not sell, rent or trade your Personal Information to third parties for their direct marketing purposes.

15. Data breach notification

15.1 Notification obligations

In the event of an eligible data breach (as defined in the Privacy Act) that is likely to result in serious harm to any individual whose Personal Information is involved, we will:

- investigate and take reasonable containment and remediation steps;
- notify affected individuals as soon as practicable, including a description of the breach, the type of information involved and recommended steps;
- notify the Office of the Australian Information Commissioner (OAIC) in accordance with the NDB Scheme; and
- where the GDPR applies, notify the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible, and the affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.

15.2 Delayed notification

Notifications may be delayed where law enforcement, regulators or security considerations reasonably require it.

16. Third-party links and services

The Service may contain links to or integrate with Third-Party Services. We are not responsible for the privacy practices or content of those services. You should review the privacy policies of any Third-Party Services before providing Personal Information to them.

17. Changes to this Policy

17.1 Updates

We may update this Policy from time to time to reflect changes to law, regulation, technology, our practices or the Service. When we do, we will revise the effective date at the top of this Policy and publish the updated version on our Website.

17.2 Material changes

For material changes that adversely affect your rights or the way we handle your Personal Information, we will give at least 30 days' notice by email to the Account Owner and, where reasonably practicable, by in-product notification, before the change takes effect.

17.3 Continued use

Continued use of the Service after a change takes effect constitutes acceptance of the revised Policy, to the extent permitted by law. If you do not agree with a material change, you may stop using the Service and cancel your Subscription before it takes effect.

18. Contact details

If you have questions, concerns or complaints about this Policy or our handling of Personal Information, please contact us:

Dexify AI Pty Ltd

ACN 698 912 882

ABN: 13 698 912 882

Trading name: Dexify AI Pty Ltd

Registered or business address: 83 Jarrett Street, Wyoming NSW 2250, Australia

Customer support: contact@dexifyai.com

Privacy enquiries: contact@dexifyai.com

Website: <https://dexifyai.com>

End of Privacy Policy.