

Privacy Policy

How AI Uniti collects, uses, stores, and discloses personal information

Document	Privacy Policy
Version	v2.0 (Final)
Effective date	23 May 2026
Supersedes	v1.x (all prior versions)
Applies to	All visitors to aiuniti.com, users of AI Uniti products, and individuals whose data is processed by AI Uniti
Regulatory basis	Privacy Act 1988 (Cth) and Australian Privacy Principles; GDPR where applicable

1. About this Privacy Policy

AI Uniti Pty Ltd (ACN 694 238 821) (AI Uniti, we, us, our) is committed to protecting the privacy of individuals whose personal information we hold. This Privacy Policy explains how we collect, hold, use, and disclose personal information, and how you may access and correct it.

This policy applies to all personal information we collect through our website (aiuniti.com), our products (Pulse Check, Signal, Unite), our APIs, and our business operations (sales, support, recruitment, and corporate functions). We comply with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). For data subjects in the European Union, the United Kingdom, and other jurisdictions with equivalent regimes, we additionally comply with the applicable provisions of the General Data Protection Regulation (GDPR) and equivalent laws.

2. Personal information we collect

We collect the following categories of personal information.

2.1 Information you provide directly

- Identity information: full name, job title, employer.
- Contact information: business email address, business phone number, business postal address.
- Account information: username, password (hashed), authentication tokens, role and permissions within your organisation.
- Commercial information: purchase orders, invoices, payment instructions (processed by our payment sub-processor).
- Communication content: messages you send to us via email, support tickets, contact forms, and live chat.

2.2 Information collected automatically

- Usage information: pages visited, features used, queries submitted, timestamps, IP address (truncated for analytics).
- Device and browser information: device type, operating system, browser, language preference.
- Cookies and similar technologies (see section 13).

2.3 Information processed on behalf of our customers

Our enterprise customers configure our products to process data they obtain from third-party online platforms (Platform-Sourced Data). That data may include public profile information, public post and comment content, and behavioural metadata relating to accounts on those platforms. We process Platform-Sourced Data as a processor on our customers' instructions, in accordance with our Data Processing Agreement and Acceptable Use Policy. We do not act as a data controller in respect of Platform-Sourced Data.

3. How we use personal information

We use personal information for the following purposes:

- to provide, maintain, and improve our products and services;
- to authenticate users and protect account security;
- to communicate with you about your account, our products, billing, support, and changes to our terms;
- to send marketing communications, where permitted by law and subject to your right to opt out;
- to comply with our legal obligations and to enforce our rights;
- to detect, prevent, and respond to fraud, abuse, and security incidents;
- to conduct internal analytics, research, and product improvement using aggregated and de-identified information.

4. Lawful basis for processing

For data subjects in jurisdictions where a lawful basis is required (including the EU and UK), we rely on the following bases:

- Performance of a contract with you or your employer;
- Compliance with a legal obligation;
- Our legitimate interests in operating, securing, and improving our business, balanced against your rights;
- Your consent, where the processing requires it (for example, marketing communications and certain cookies).

5. Disclosure and sharing

We disclose personal information only to:

- our sub-processors, listed in the Subprocessor Disclosure, who process information on our behalf under contract;

- professional advisers (legal, accounting, audit) bound by confidentiality;
- law enforcement or regulators where we are required by law to do so;
- a successor entity in connection with a merger, acquisition, financing, or sale of all or substantially all of our assets, subject to equivalent privacy commitments;
- with your consent, in any other case.

We do not sell personal information. We do not disclose personal information to third parties for their own direct marketing purposes.

6. Cross-border data flows and hosting

AI Uniti operates a customer-selectable hosting model. The default deployment region is Amazon Web Services Asia Pacific (Sydney) (ap-southeast-2). Customers may elect, by written agreement, to be deployed in an alternative cloud region or in a customer-managed on-premises environment. Where data is processed in a region other than Australia, we ensure that the processing is subject to contractual safeguards equivalent to the Australian Privacy Principles and, where applicable, to GDPR-compliant transfer mechanisms (Standard Contractual Clauses or an adequacy decision).

Personal information processed in connection with our corporate operations (sales, marketing, support, billing) may be processed by our corporate sub-processors in the United States and the European Union. See the Subprocessor Disclosure for the current list.

7. Security

We implement technical and organisational measures designed to protect personal information against unauthorised access, alteration, disclosure, or destruction. These measures are described in the Information Security Policy and include encryption in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent), role-based access control, multi-factor authentication for administrative access, security logging and monitoring, vulnerability management, and personnel security controls. We are pursuing SOC 2 Type I certification, with completion targeted for Q4 FY26.

8. Data retention

We retain personal information for no longer than is necessary for the purposes for which it was collected, subject to legal obligations. Specific retention windows are as follows.

Category	Retention window	Rationale
Account and contact information	Duration of customer relationship + 7 years	Australian tax and corporate record-keeping obligations
Authentication credentials and tokens	Until rotation; revoked tokens deleted within 30 days	Operational security
Raw third-party Platform-Sourced Data	90 days from ingestion	Operational minimum; restricts re-use and aligns with strictest source-platform terms
Aggregated and de-identified behavioural indicators	24 months maximum	Pattern detection over time; data is not personal once de-identified

Category	Retention window	Rationale
Per-account scores and per-account derived data	Duration of customer subscription only; deleted on termination within 30 days	Customer-tenant data; deletion-on-termination commitment in DPA
System logs, audit trails, security telemetry	12 months	Incident investigation and audit
Marketing data and CRM records	Until consent withdrawal + 30 days	Australian Spam Act and GDPR compliance
Billing and transaction records	7 years	Australian tax law

9. Sensitive personal characteristics

AI Uniti will not infer, derive, model, or report the following Sensitive Personal Characteristics about any Identifiable Individual on the basis of Platform-Sourced Data: health information, political opinion or political association, sexual orientation or sexual practices, religious belief, philosophical belief, racial or ethnic origin, membership of a trade union or professional or trade association, criminal record, biometric data used for identification, or genetic data.

This commitment is absolute. It applies regardless of the technical feasibility of such inference, regardless of whether the inference is requested by a customer, and regardless of whether the inference is intended to be used for adverse decision-making.

10. De-anonymisation and identity matching

AI Uniti will not de-anonymise users of any third-party online platform whose terms of service prohibit de-anonymisation. AI Uniti will not match identifiers from any such platform to identifiers, accounts, or identities on any other platform or in any off-platform data set, including but not limited to email addresses, phone numbers, government identifiers, and biometric identifiers.

For platforms whose terms do not expressly prohibit identity matching, AI Uniti's cross-platform identity graph operates only on signals expressly permitted by the relevant platform's terms, and only for the purpose of detecting coordinated inauthentic behaviour.

11. Your rights

Subject to applicable law, you have the following rights in relation to personal information we hold about you:

- Access: you may request a copy of the personal information we hold about you.
- Correction: you may request correction of inaccurate or incomplete information.
- Deletion: you may request deletion of your personal information, subject to our legal obligations to retain it.
- Restriction or objection: you may request that we restrict processing or object to processing where the law gives you that right.
- Portability: where the GDPR applies, you may request a portable copy of information you provided to us.
- Withdraw consent: you may withdraw consent for processing that depends on consent (such as marketing).

- Complaint: you may complain to us and, if unresolved, to the Office of the Australian Information Commissioner (oaic.gov.au) or the equivalent regulator in your jurisdiction.

To exercise any of these rights, contact us at privacy@aiuniti.com. We will respond within 30 days, or such shorter period as required by applicable law.

12. Direct marketing

Where we send you marketing communications, you may opt out at any time using the unsubscribe link in the communication or by emailing privacy@aiuniti.com. We comply with the Spam Act 2003 (Cth) and equivalent legislation in jurisdictions where we send marketing communications.

13. Cookies and tracking technologies

Our website uses essential cookies required for the site to function, and analytics cookies that help us understand how visitors interact with the site. You can manage cookies through your browser settings. We do not use third-party advertising cookies or behavioural advertising tracking.

14. Children

AI Uniti products are not directed at children. We do not knowingly collect personal information from children under 16. If we become aware that we have collected information from a child under 16, we will delete it.

15. Changes to this policy

We may update this Privacy Policy from time to time. Material changes will be notified to customers in writing at least 30 days before they take effect, and on our website. The effective date at the top of this document indicates when it was last updated.

16. Contact us

Privacy enquiries and rights requests: privacy@aiuniti.com.

Postal: AI Uniti Pty Ltd, Brisbane, Queensland, Australia [registered address to be confirmed].

If you are not satisfied with our handling of your complaint, you may contact the Office of the Australian Information Commissioner (oaic.gov.au, 1300 363 992) or the equivalent regulator in your jurisdiction.

End of Privacy Policy v2.0. Effective 23 May 2026.