DATA PROCESSING AGREEMENT

Controller to processor terms for customer personal data processed by AI Uniti

What changed in v2.1

Section 10 (Sub-processors) is tightened in two respects. A customer objection to a new Sub-processor must now be raised within the 30-day notice period, and the consequence of termination is stated explicitly as a pro-rata refund of prepaid Fees rather than the undefined phrase "without penalty". No other section is changed. Section 13 (International transfers) already provides for Standard Contractual Clauses and the UK International Data Transfer Addendum, and is unchanged.

Document	Data Processing Agreement (DPA)
Version	v2.1 (Final)
Effective date	27 August 2026
Supersedes	v2.0 dated 23 May 2026, and all prior versions
Applies to	All customers of AI Uniti where AI Uniti processes Personal Data on the customer's behalf
Status	Incorporated by reference into all Order Forms and the EULA

1. Background and scope

This Data Processing Agreement (DPA) is entered into between the customer identified in the applicable Order Form (Customer) and AI Uniti Pty Ltd (ACN 694 238 821) (AI Uniti). It applies whenever AI Uniti processes Personal Data on behalf of the Customer in connection with the Services.

This DPA supplements the End User Licence Agreement (EULA) and the Order Form. To the extent of any conflict in respect of the processing of Personal Data, this DPA prevails.

2. Definitions

Capitalised terms used in this DPA have the meaning given in the EULA, or, where not so defined, the meanings below.

- Applicable Data Protection Laws means the Privacy Act 1988 (Cth) and the Australian Privacy Principles; the General Data Protection Regulation (Regulation (EU) 2016/679) and any equivalent law of the United Kingdom; and any other data protection or privacy law applicable to the processing.
- Customer Personal Data means Personal Data processed by AI Uniti on behalf of the Customer under the Services.
- Data Subject, Personal Data, Processing, Controller and Processor have the meanings given in the GDPR.
- Platform-Sourced Data means data obtained from any third-party online platform processed by the Services.
- Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
- Sub-processor means any third party engaged by AI Uniti to process Customer Personal Data.

3. Roles of the parties

In relation to Customer Personal Data, the Customer is the Controller (or, where the Customer is itself a processor for an upstream controller, the Customer warrants it has the necessary authority and the relevant flow-down terms) and AI Uniti is the Processor. AI Uniti will process Customer Personal Data only on the Customer's documented instructions, including those set out in this DPA, the EULA, the Order Form, and any subsequent written instructions issued by the Customer.

4. Subject matter, duration, nature and purpose

Subject matter: provision of the Services as described in the Order Form. Duration: for the term of the Order Form, plus any post-termination retention period expressly permitted by this DPA. Nature: collection, storage, structuring, analysis, and disclosure to the Customer of Personal Data, including Platform-Sourced Data, for the purpose of coordinated inauthentic behaviour detection, platform integrity, narrative risk monitoring, and abuse defence. Categories of Data Subjects and Personal Data: see Schedule 1.

5. Customer's obligations

The Customer warrants that:

- it has, and will maintain throughout the term, all necessary rights, consents and authorisations to provide or instruct the processing of Customer Personal Data;
- its instructions to AI Uniti comply with Applicable Data Protection Laws;
- any Platform-Sourced Data it instructs AI Uniti to process is obtained in compliance with the terms of service of the source platform and with Applicable Data Protection Laws;
- it will not instruct AI Uniti to process Customer Personal Data in any manner that would cause AI Uniti to breach this DPA, the AUP, or Applicable Data Protection Laws.

6. AI Uniti's processing obligations

AI Uniti will:

- process Customer Personal Data only on the Customer's documented instructions, and only for the purposes set out in section 4 and the Order Form;
- ensure that personnel authorised to process Customer Personal Data are bound by appropriate confidentiality obligations;
- implement and maintain technical and organisational measures meeting the requirements of section 9 (Security);
- engage Sub-processors only in accordance with section 10;
- assist the Customer, taking into account the nature of the processing, in responding to Data Subject requests (section 11) and in fulfilling the Customer's obligations under Applicable Data Protection Laws;
- notify the Customer of Personal Data Breaches in accordance with section 12;
- make available all information necessary to demonstrate compliance with this DPA, and contribute to audits, in accordance with section 15;
- delete or return Customer Personal Data at the end of the provision of the Services in accordance with section 16;
- promptly inform the Customer if, in AI Uniti's opinion, an instruction from the Customer infringes Applicable Data Protection Laws.

7. Restrictions on AI Uniti's use of Customer Personal Data

AI Uniti will not, except as expressly permitted by this DPA or the EULA:

- use Customer Personal Data, or any data derived from it, for AI Uniti's own purposes;
- use Customer Personal Data, or any data derived from it, to train, fine-tune, or otherwise improve any foundation model, large language model, or other general-purpose AI model;
- where the Customer Personal Data is or includes Platform-Sourced Data, use that data to train, fine-tune, or improve any foundation model or large language model, except with the prior written approval of the source platform;
- disclose or transfer Customer Personal Data to any third party other than as permitted by sections 10 (Sub-processors) and 13 (International transfers).

8. Confidentiality

AI Uniti will treat Customer Personal Data as Confidential Information of the Customer and will not disclose it except as permitted by this DPA or required by law. Personnel with access to Customer Personal Data are bound by written confidentiality obligations.

9. Security measures

AI Uniti will implement and maintain the technical and organisational measures set out in Schedule 2 and in the Information Security Policy, designed to ensure a level of security appropriate to the risk. Measures include encryption in transit and at rest, role-based access control, multi-factor authentication, security logging and monitoring, vulnerability management, incident response procedures, and personnel security.

AI Uniti is pursuing SOC 2 Type I certification, with completion targeted for Q4 FY26. Upon completion, AI Uniti will make the audit report available to the Customer under NDA on request.

10. Sub-processors

Amended in v2.1. The Customer authorises AI Uniti to engage the Sub-processors listed in the Subprocessor Disclosure for the Services. AI Uniti will:

- impose written obligations on each Sub-processor that are no less protective than this DPA in respect of Customer Personal Data;
- remain liable for the acts and omissions of its Sub-processors as if performed by AI Uniti itself;
- notify the Customer at least 30 days before adding or replacing a Sub-processor whose processing affects Customer Personal Data, by updating the Subprocessor Disclosure and notifying the Customer by email if the Customer has subscribed to such notifications;
- where the Customer reasonably objects to a new or replacement Sub-processor on data protection grounds, and raises that objection in writing within the 30-day notice period referred to above, work with the Customer in good faith to identify an alternative. If no alternative is found within a further 30 days, the Customer may terminate the affected Order Form in respect of the affected Services, and AI Uniti will refund prepaid Fees for those Services on a pro-rata basis calculated from the effective date of termination. This right does not apply to Sub-processors listed in the Subprocessor Disclosure at the date the Customer signs the Order Form, which the Customer authorises on signature.

11. Data subject requests

Where AI Uniti receives a request from a Data Subject in relation to Customer Personal Data, AI Uniti will, unless prohibited by law, refer the request to the Customer without responding to the Data Subject directly. AI Uniti will assist the Customer in responding to such requests, taking into account the nature of the processing and the information available to AI Uniti.

12. Personal Data Breach notification

AI Uniti will notify the Customer of any Personal Data Breach affecting Customer Personal Data without undue delay and in any event within 72 hours of becoming aware. The notification will include, to the extent known at the time:

- the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and records concerned;
- the likely consequences of the breach;
- the measures taken or proposed to address the breach and mitigate its effects;
- the contact details of AI Uniti's incident response lead.

AI Uniti will provide further information promptly as it becomes available, and will cooperate with the Customer in any related investigation or regulator notification.

13. International transfers

Where processing involves the transfer of Customer Personal Data to a country other than the country of origin, AI Uniti will ensure that an appropriate transfer mechanism applies. For transfers from the European Economic Area, the United Kingdom, or Switzerland to a third country that is not the subject of an adequacy decision, AI Uniti will execute the relevant Standard Contractual Clauses (and, where applicable, the UK International Data Transfer Addendum), which are incorporated by reference into this DPA on signature.

For clarity, media submitted by the Customer for deepfake detection is transferred to Reality Defender, Inc. in the United States. That transfer is made under the mechanisms described in this section and is recorded in the Subprocessor Disclosure.

14. Hosting region and deployment model

AI Uniti operates a customer-selectable hosting model. The default deployment region is Amazon Web Services Asia Pacific (Sydney) (ap-southeast-2). The Customer may elect, by Order Form or written variation, to deploy the Services in:

- an alternative AWS region required by the Customer (subject to availability and any incremental fee specified in the Order Form);
- another cloud provider region supported by AI Uniti from time to time;
- a Customer-managed on-premises environment, where the Customer hosts the Services on its own infrastructure under a separate self-hosted licence.

Where the Customer elects an on-premises deployment, the Sub-processor list in respect of the hosting layer reduces accordingly, and the Customer is responsible for the security of the underlying infrastructure. AI Uniti remains responsible for the application layer. Sub-processors engaged at the application layer, including deepfake detection, continue to apply in all deployment models.

15. Audit rights

AI Uniti will, on reasonable written request, provide the Customer with the most recent third-party audit report (including SOC 2 once available) and reasonable additional information to demonstrate compliance with this DPA. Where the Customer reasonably considers that such information is insufficient, the Customer may, no more than once in any twelve-month period and at its own cost, audit AI Uniti's processing of Customer Personal Data, subject to AI Uniti's reasonable security, confidentiality and operational requirements. AI Uniti and the Customer will agree the scope, timing and duration of any such audit in advance.

16. Deletion or return of Customer Personal Data

On termination of the applicable Order Form, or on the Customer's written request at any time during the term, AI Uniti will, at the Customer's election:

- delete all Customer Personal Data in AI Uniti's possession or control; or
- return all Customer Personal Data to the Customer in a structured, commonly used, machine-readable format, and then delete it.

Deletion will be completed within 30 days of termination or written request, and will cover:

- raw Customer Personal Data, including Platform-Sourced Data and any data derived from the Customer's tenant;
- per-account scores and per-account derived data attributable to the Customer's tenant;
- any model artefacts trained on Customer Personal Data from the Customer's tenant;
- backups, within the standard backup rotation cycle, which is no longer than 90 days from termination.

AI Uniti will retain aggregated and de-identified data only where the data no longer constitutes Personal Data and where retention is consistent with the AUP and this DPA. AI Uniti will, on written request, provide the Customer with a certificate of deletion signed by an officer of AI Uniti.

AI Uniti may retain Customer Personal Data only to the extent required by law, and only for the period required by that law. Such retention is subject to the confidentiality and security obligations of this DPA.

17. Liability

The liability of each party under this DPA is governed by, and limited in accordance with, the liability provisions of the EULA. Nothing in this DPA limits liability that cannot be limited under Applicable Data Protection Laws.

18. Term and survival

This DPA takes effect on the effective date of the Order Form and continues for so long as AI Uniti processes Customer Personal Data. Sections 12 (Breach), 15 (Audit), 16 (Deletion) and 17 (Liability) survive termination.

19. Governing law and jurisdiction

This DPA is governed by the laws of New South Wales, Australia. The parties submit to the non-exclusive jurisdiction of the courts of New South Wales.

Schedule 1: Description of processing

Subject matter: provision of the Services. Duration: for the term of the Order Form.

Nature and purpose of processing: detection of coordinated inauthentic behaviour, narrative manipulation and platform abuse; deepfake detection on media submitted by the Customer; provision of analytics and alerting to the Customer; storage and processing of Platform-Sourced Data.

Categories of Data Subjects

- the Customer's authorised users of the Services;
- individuals whose public information appears on third-party online platforms within the scope of the Customer's queries;
- individuals appearing in media submitted by the Customer for deepfake detection.

Categories of Personal Data

- authentication and account information of the Customer's authorised users;
- publicly available content from third-party online platforms, including posts, comments and profile information;
- behavioural metadata associated with public accounts on those platforms (post timing, posting patterns, network connections);
- media submitted by the Customer for deepfake detection, being images, video, audio and text files, and any Personal Data contained in that media;
- derived analytical outputs (coordination scores, campaign indicators, detection results) attributable to public accounts or submitted media.

AI Uniti will not process special categories of Personal Data (Sensitive Personal Characteristics) about Identifiable Individuals, in accordance with section 7 and the AUP.

Schedule 2: Technical and organisational measures

AI Uniti implements the technical and organisational measures described in the Information Security Policy (current version), including:

- Access control: role-based access control with least-privilege defaults; multi-factor authentication for administrative access; quarterly access reviews.
- Encryption: TLS 1.2 or higher for data in transit; AES-256 or equivalent for data at rest; key management via managed key services in the deployment region.
- Network security: segmentation between production and non-production environments; perimeter and host-based controls; default-deny ingress.
- Logging and monitoring: security event logging with 12-month retention; anomaly detection; on-call security response.

- Vulnerability management: dependency scanning; quarterly external penetration testing once the SOC 2 programme is underway; rapid patching of critical vulnerabilities.
- Personnel security: background checks for personnel with production access; security training on hire and annually; signed confidentiality and acceptable use agreements.
- Incident response: documented incident response plan; tabletop exercises annually; 72-hour Personal Data Breach notification commitment.
- Business continuity: documented disaster recovery procedures; backup integrity testing.
- Sub-processor security: due diligence on engagement; contractual flow-down of security obligations; ongoing monitoring.

Detailed descriptions and current control attestations are maintained in the Information Security Policy.

Schedule 3: Sub-processors

The current list of Sub-processors is maintained in the AI Uniti Subprocessor Disclosure (current version), incorporated by reference.

Version history

Version	Date	Summary
v2.1	27 August 2026	Section 10 objection window and refund consequence clarified. Deepfake detection recognised in sections 13, 14 and Schedule 1.
v2.0	23 May 2026	Full controller to processor terms. Superseded.
v1.x	Prior	Superseded.

End of Data Processing Agreement v2.1. Effective 27 August 2026.