

DATA PROCESSING ADDENDUM

Article 28 GDPR and the Privacy Act 1988 (Cth) | Template for execution with clients
Alfred AI Agent Services Pty Ltd (AlfredAI.bot)

DOCUMENT CONTROL

Document ID: DPA-CLIENT | **Version:** 2.3 | **Classification:** Contractual

Owner: Privacy Lead (Alex Tandrau) | **Approver:** CEO (William Zhang)

Effective date: 2026-09-29 (v2.3); v2.2 effective 2026-09-28; v2.1 effective 2026-09-26; v2.0 effective 2026-08-13

Change history: v1.0 — drafted to the Privacy Act 1988 (Cth) only, unexecuted, with no Article 28(3) terms, no audit right, no infringing-instruction duty, and a data residency assertion that did not match the technical position. v2.0 2026-08-13 — reissued to carry the full Article 28(3) terms, the audit and information right, the duty to inform the controller of an infringing instruction, the sub-processor regime, and the hosting and transfer position as it actually operates (Stage 2 GDPR NC 1) v2.1 2026-09-26 — Annex 2 network statement corrected: the clause previously read that the application and data layers have “no route to the internet”, which was accurate for inbound traffic only. Outbound access is permitted through a managed gateway for updates and provider calls, as the signed network segregation statement NET-01 v2.3 records and as exception EXC-2026-03 governs. Corrected following independent privacy audit AUD-PRIV-2026-01, finding F-09. No other clause changed. v2.2 2026-09-28 — Annex 2 prompt-handling measure corrected: it previously read “minimisation and redaction of personal data placed in prompts”. No redaction step exists in the path by which prompts are sent to model providers; a production capture of the request body on 25 September 2026 shows message content sent as entered, with no account, user or session identifier attached. The measure now states minimisation only, matching Privacy Notice v2.1 (independent privacy audit AUD-PRIV-2026-01, finding F-09). No other clause changed. v2.3 2026-09-29 — Annex 1 completed for the shared platform: the nature and purpose of the processing, the categories of personal data and of data subjects, special categories, the hosting location, and the retention and deletion timetable, which previously were left to be completed per engagement, so that clients on the shared platform, who accept this Addendum through the Terms, hold a complete Article 28(3) description. An engagement-specific Annex 1 replaces it where agreed. Annex 3 now sets out the list of sub-processors in force and states where the current list is published. The execution block is replaced by an acceptance clause: the Addendum is accepted with the Terms, and a copy signed by both parties is provided on request. Clause 4(b) states the hosting of the DeepSeek models as it operates: through OpenRouter, on hosts that include providers in China, restricted to providers with a no-data-retention policy. No other clause changed.

1. PARTIES, SCOPE AND ROLES

- a. This Addendum forms part of the services agreement between the client (the "Controller") and Alfred AI Agent Services Pty Ltd, ABN 62 684 936 525 (the "Processor"), and governs the Processor's processing of personal data on the Controller's behalf.
- b. Where the General Data Protection Regulation (EU) 2016/679 applies to the Controller's processing, this Addendum applies as the Article 28(3) agreement. The Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles apply in addition, and nothing in this Addendum reduces the protection given by either instrument. Where the two conflict, the higher standard applies.
- c. The Controller determines the purposes and means of the processing. The Processor processes personal data only to provide the services and only on the Controller's documented instructions.
- d. Annex 1 sets out the subject matter, duration, nature and purpose of the processing, the categories of personal data and of data subjects. Annex 2 sets out the technical and organisational measures. Annex 3 sets out the authorised sub-processors.

2. PROCESSOR OBLIGATIONS UNDER ARTICLE 28(3)

- a. Documented instructions. The Processor processes personal data only on the documented instructions of the Controller, including in relation to transfers of personal data to a third country, unless required to do otherwise by law; in that case the Processor informs the Controller before processing, unless the law prohibits that information on important grounds of public interest. (Article 28(3)(a).)
- b. Confidentiality. The Processor ensures that every person authorised to process the personal data is subject to a duty of confidentiality, whether that person is an officer of the Processor, engaged under a direct contract, or provided through the Processor's subcontracting arrangement. (Article 28(3)(b).)

- c. Security. The Processor implements the technical and organisational measures required by Article 32, as described in Annex 2 and evidenced by the Processor's ISO/IEC 27001 information security management system. (Article 28(3)(c).)
- d. Sub-processors. The Processor engages sub-processors only under the conditions in clause 3 and imposes on each sub-processor, by written contract, data protection obligations equivalent to those in this Addendum. The Processor remains liable to the Controller for the performance of each sub-processor. (Article 28(3)(d), 28(2) and 28(4).)
- e. Data subject rights. The Processor assists the Controller, by appropriate technical and organisational measures and so far as is possible, in fulfilling requests to exercise rights under Chapter III, and refers any request it receives directly to the Controller without responding to it substantively. (Article 28(3)(e).)
- f. Assistance with compliance. The Processor assists the Controller in ensuring compliance with Articles 32 to 36, taking into account the nature of the processing and the information available to the Processor. This includes notifying the Controller without undue delay and in any event within 24 hours of becoming aware of a personal data breach affecting the Controller's personal data, with the information the Controller needs to meet its own notification obligations, and supporting the Controller's data protection impact assessments and prior consultations. (Article 28(3)(f).)
- g. Deletion or return. On termination or expiry of the services, and at the Controller's choice, the Processor deletes or returns the personal data and deletes existing copies, unless a legal obligation requires storage. Deletion covers the production database, the cache, object storage, the vector index and backups, on the timetable in the Data Deletion and Return Procedure, and the Processor provides written confirmation. (Article 28(3)(g).)
- h. Information and audit. The Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 and allows for and contributes to audits, including inspections, by the Controller or an auditor mandated by the Controller. The Processor may satisfy an audit request by providing its current ISO/IEC 27001 certificate, its most recent penetration test summary and its completed security questionnaire; where those do not answer the Controller's question, the Controller may audit on 30 days' notice, no more than once in any 12 months except following a personal data breach, during business hours, subject to confidentiality and without access to other clients' data. (Article 28(3)(h).)
- i. Infringing instructions. The Processor informs the Controller immediately if, in its opinion, an instruction infringes the General Data Protection Regulation or another applicable data protection provision, and may suspend the affected processing until the instruction is confirmed or withdrawn. (Article 28(3), final paragraph.)

3. SUB-PROCESSORS

- a. The Controller gives general written authorisation for the Processor to engage the sub-processors listed in Annex 3.
- b. The Processor notifies the Controller of any intended addition or replacement of a sub-processor at least 30 days in advance, so that the Controller has the opportunity to object. Notification is given under the Sub-processor Change Communication Plan.
- c. If the Controller objects on reasonable data protection grounds, the parties discuss in good faith. If no resolution is reached, the Controller may terminate the affected part of the services without penalty.
- d. The list in Annex 3 reflects the Processor's Sub-processor Register, which records for each sub-processor the processing purpose, the categories of personal data, the hosting location and the transfer mechanism.

4. INTERNATIONAL TRANSFERS

- a. The Processor hosts the shared platform in the United States (Amazon Web Services, us-east-1) and hosts per-client custom deployments in Australia (Oracle Cloud, Sydney), including a dedicated deployment for clients requiring Australian data residency. Where a client requires Australian data residency, that requirement is met by a dedicated deployment and is recorded in Annex 1.

b. Certain sub-processors are located in the United States. DeepSeek models are served through OpenRouter, which routes each request to one of several hosting providers; for these models those providers include hosts in the United States, Europe and China. Requests are restricted to providers with a no-data-retention policy, which do not retain or train on the data submitted, and DeepSeek's own API is not used. The recipients, the countries involved and the transfer mechanism relied upon for each are recorded in Annex 3 and in the Processor's International Data Transfer Assessment.

c. Where the Controller's processing is subject to Chapter V of the General Data Protection Regulation, transfers are made on the Standard Contractual Clauses, or on provider data processing terms that incorporate them, together with the supplementary measures recorded in the transfer impact assessment for that recipient. The Processor provides a copy of the safeguards on request.

d. No statement of data residency is made in this Addendum that is not reflected in Annex 1 for the particular engagement.

5. ANNEX 1 — THE PROCESSING

Item	Shared platform (self-serve subscription). This Annex 1 applies to every client on the shared platform unless an engagement-specific Annex 1 is agreed in writing.
Subject matter and duration	The provision of the services for the term of the services agreement, and for the period needed to delete or return the personal data on termination.
Nature and purpose of the processing	Processing on the Client's documented instructions to provide the features the Client enables: • AI chatbots and assistants over the Client's content: knowledge bases, visitor conversations and lead capture, document embeddings; • mailbox automation: reading, classifying, drafting and sending email from mailboxes the Client connects; • meeting and call recording, transcription and summarisation; • outbound engagement campaigns the Client instructs: AI voice calls, SMS/WhatsApp and email to contact lists the Client provides; • lead generation and enrichment of business prospects matching the Client's criteria; • delegated access to the Client's business accounts (OAuth) so that the automations can act as instructed.
Categories of personal data	Account identifiers and business contact details (name, email, phone, job title); chat messages and uploaded documents; email bodies, attachments and metadata; call and meeting recordings and transcripts; message content and delivery status; captured leads; OAuth tokens for accounts the Client connects.
Categories of data subjects	The Client's staff and users; the Client's website visitors and customers; the Client's correspondents, meeting and call participants; contacts and leads the Client provides; business prospects identified for the Client; individuals referred to in the Client's content.
Special categories of data, if any, and the additional restrictions applied	None intended. The services are not designed for special categories of personal data or data on criminal convictions, and the Client should not submit them. Where the Client needs such data processed, it is agreed in an engagement-specific Annex 1 before processing starts, with the additional safeguards stated there.
Hosting location for this engagement, and any Australian data residency requirement	Shared platform: United States (Amazon Web Services, us-east-1), with the sub-processors and transfer mechanisms in Annex 3. No Australian data residency requirement applies to the shared platform. A Client that requires Australian data residency is served from a

	dedicated deployment in Australia (Oracle Cloud, Sydney), recorded in an engagement-specific Annex 1.
Retention period and the deletion timetable on termination	During the term: conversation content is kept for the retention window the Client sets on each chatbot (7, 30, 60, 90, 180 or 365 days) and purged automatically on expiry; where the Client sets no window, it is kept until the Client deletes it or the services end. Other content is kept until the Client deletes it or the services end. On termination: at the Client's choice, the personal data is returned or deleted from the production database, object storage and vector index, and written confirmation is given (clause 2(g)). Copies in backups expire on the backup schedule: production database snapshots after 7 days, chatbot backups after up to 90 days.
Controller contact for data protection matters	The contact the Client records on its account.
Processor contact for data protection matters	Privacy Lead, Alfred AI Agent Services Pty Ltd — enquiry@alfredai.bot

6. ANNEX 2 — TECHNICAL AND ORGANISATIONAL MEASURES

- An information security management system certified to ISO/IEC 27001, with the Statement of Applicability available on request.
- Encryption in transit (TLS) and at rest for the database, object storage and backups.
- Network segregation: the web, application and data layers are in separate subnets. The application and data layers have no inbound path from the internet and are not publicly addressable. Outbound access from those layers is permitted only through a managed gateway, for software updates and for calls to the service providers listed in the Processor's sub-processor register, and is monitored. Per-client deployments have no network path to one another.
- Access control on the principle of least privilege, unique named accounts, enforced multi-factor authentication, quarterly privileged access review and semi-annual full access review.
- Screening of every individual who performs work on the systems, proportionate to the role, with enhanced verification for privileged, production and repository access.
- Vulnerability management with defined remediation service levels, static, dependency and dynamic scanning, and an annual independent penetration test.
- Logging, monitoring and threat detection across both clouds, with a documented incident response and breach notification process.
- Backups with restore testing at least annually per environment.
- Minimisation of personal data placed in prompts sent to model providers, per the AI Data Minimisation Standard: prompts carry no account, user or session identifier, and the content the Controller's users enter is not redacted before it is sent.

7. ANNEX 3 — AUTHORISED SUB-PROCESSORS

The current list, with the processing purpose, the categories of personal data, the hosting location and the transfer mechanism for each entry, is maintained in the Processor's Sub-processor Register and is provided with this Addendum at execution and on request thereafter. The published list and the register are reconciled whenever

either changes, so that the list given to the Controller and the register the Processor operates from are the same set. The list in force at the date of this version is set out below. Any later change is notified under clause 3(b), and the current list is published at <https://app.alfredai.bot/policy>.

Sub-processor	What it does	Location
Amazon Web Services	Cloud hosting, storage and managed databases for the shared platform	United States (us-east-1)
Oracle Cloud	Dedicated per-client hosting, including deployments for clients requiring Australian data residency	Australia (Sydney)
Microsoft Azure	Client mailbox and document integration	Per client — recorded in the register
Google Workspace	Email, identity and document services	United States
GitHub	Source code management	United States
OpenRouter	AI model routing, including the Google Gemini and DeepSeek models reached through it	United States; for DeepSeek models, routed hosts include providers in the United States, Europe and China
OpenAI	AI model inference	United States
Anthropic	AI model inference	United States
xAI	AI model inference	United States
Pinecone	Vector search over document and conversation content	United States
Vapi	Voice assistant platform	United States
Twilio	Telephony and messaging	United States
ElevenLabs	Speech synthesis	United States
Recall.ai	Meeting recording and transcription	United States
Apify	Public web retrieval for business development	United States
Apollo	Business contact data for business development	United States
Stripe	Payment processing	United States
Xero	Financial administration and invoicing	New Zealand
Slack	Internal collaboration	United States
Dropbox	Document storage and transfer	United States
MailerSend	Transactional and outreach email delivery	United States
Meta (WhatsApp Business Platform)	Delivery of WhatsApp messages to and from client contacts	Ireland (WhatsApp Ireland Limited), with onward transfer to the United States
Bitly	Link shortening for shared chatbot links	United States
Ignition	Reporting over the client's proposals and engagements, under the client's authorisation	United States and Australia
Apple	In-app purchase receipt validation for the mobile app	United States
Better Stack	Uptime monitoring of the public endpoints	United States
Cloudflare	Network and DNS protection — being adopted; not yet processing any personal data. Listed here as advance notice under clause 3(b) of the Data Processing Addendum.	United States, once live
Expo	Mobile application build and delivery	United States
Pipedrive	Customer relationship management	Australia
Vanta	Compliance monitoring	United States

8. ACCEPTANCE

This Addendum forms part of the Terms and is accepted with them; no separate signature is required. A copy signed by both parties is provided on request.

APPROVAL FOR ISSUE (v2.3)

Approved by: William Zhang, Chief Executive Officer

Signature: _____

A handwritten signature in black ink, consisting of several loops and a final horizontal stroke.

Date: _____29.09.2026_____