Data Processing Agreement

Processor: Salim Zakkour trading as OpsBots **ABN:** 22 838 356 145 **Version:** 1.1

Effective: 19 March 2026 **Contact:** hello@opsbots.com.au

This Data Processing Agreement ("DPA") forms part of the Service Agreement between the Client ("Controller") and **Salim Zakkour trading as OpsBots (ABN 22 838 356 145)** ("Processor") for the provision of AI-powered MSP support services.

This DPA governs the processing of personal information by the Processor on behalf of the Controller in accordance with the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**.

1. Definitions

- **"Personal Information"** has the meaning given in the Privacy Act 1988 (Cth).
- **"Controller"** means the MSP client who determines the purposes and means of processing personal information.
- **"Processor"** means Salim Zakkour trading as OpsBots (ABN 22 838 356 145), who processes personal information on behalf of the Controller.
- **"Sub-processor"** means any third party engaged by the Processor to process personal information on behalf of the Controller.
- **"Data Breach"** means an eligible data breach as defined in Part IIIC of the Privacy Act 1988 (Cth).
- **"Services"** means the AI-powered IT support automation services provided by the Processor under the Service Agreement.

2. Scope and Purpose

2.1 Purpose of Processing

The Processor processes personal information solely for the purpose of delivering the Services to the Controller, including AI-powered ticket classification, response generation, escalation, and reporting.

2.2 Duration

This DPA is effective for the duration of the Service Agreement and for the period required to complete any post-termination data handling obligations.

2.3 Types of Personal Information Processed

- Business documents and operational records
- Communications (email, chat, support tickets)
- Task descriptions and workflow metadata
- Customer contact information (names, email addresses, phone numbers)
- Technical identifiers (IP addresses, device IDs, session tokens)
- Service usage data and analytics
- Authentication credentials (hashed/encrypted)

2.4 Categories of Data Subjects

- Controller's employees and contractors
- Controller's end-user clients whose data appears in support tickets
- Controller's business contacts

3. Processor Obligations

- Process personal information only on documented instructions from the Controller, unless required by law to do otherwise.
- Ensure that persons authorised to process personal information have committed to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (see Section 6).
- Not engage another processor (sub-processor) without prior written authorisation of the Controller (see Section 5).
- Assist the Controller in responding to requests from individuals exercising their rights under the Privacy Act 1988.
- Make available to the Controller all information necessary to demonstrate compliance with this DPA.
- At the Controller's choice, delete or return all personal information to the Controller after the end of the provision of Services, and delete existing copies unless required by law to retain.

4. Data Minimisation

- The Processor shall only process personal information that is **reasonably necessary** for the delivery of the Services.
- The Processor shall not retain personal information longer than necessary for the purposes of processing. Retention periods are governed by the Processor's Privacy Policy (v5.0), Section 11.3.
- The Processor shall de-identify or delete personal information when it is no longer needed for any purpose permitted under the APPs or this DPA.

5. Sub-processors

5.1 Authorised Sub-processors

Sub-processor	Location	Purpose	Data Retained?
Anthropic (Claude API)	United States	AI-powered ticket classification and natural language processing	No — transient processing only
Self-hosted infrastructure	New South Wales, Australia	Primary data storage, task queues, operational data	Yes — under Processor's direct control

5.2 Sub-processor Changes

The Processor shall notify the Controller in writing at least **30 days** before engaging any new sub-processor or changing an existing sub-processor. The Controller may object to the appointment of a new sub-processor on reasonable grounds related to data protection. If the objection is not resolved within 14 days, the Controller may terminate the affected Services.

5.3 Sub-processor Obligations

Where the Processor engages a sub-processor, it shall impose data protection obligations no less protective than those in this DPA. The Processor remains fully liable to the Controller for the performance of the sub-processor's obligations.

6. Security Measures

The Processor implements and maintains the following technical and organisational measures:

6.1 Technical Controls

- **Encryption in transit:** All data transmitted via TLS 1.2+ encrypted connections.
- **Encryption at rest:** Data at rest is encrypted using AES-256 encryption. API keys and credentials are stored in encrypted vaults; full disk encryption on all server hardware.

- **Access control:** Role-based access with tiered authority levels and least-privilege principles.
- **Network security:** Private network (Tailscale VPN) for all inter-service communications. No public internet exposure of management interfaces.
- **Authentication:** SSH key-based access; multi-factor authentication for administrative functions.
- **Monitoring:** Automated fleet health monitoring, anomaly detection, and audit logging.

6.2 Organisational Controls

- **Data isolation:** Strict separation of data between MSP clients. No cross-client data access.
- **Audit logging:** All system actions logged with timestamps for accountability and forensic analysis.
- **Incident response:** Documented data breach response procedures (see Section 9).
- **Personnel:** All persons with access to personal information are bound by confidentiality obligations.

7. Data Protection Impact Assessment (DPIA)

- The Processor shall conduct Data Protection Impact Assessments for any new processing activities that are likely to result in **high risk** to the rights and freedoms of individuals.
- The results of DPIAs shall be made available to the Controller upon written request.
- Where a DPIA indicates that processing would result in high risk without mitigation measures, the Processor shall consult with the Controller before proceeding with the processing.

8. Audit Rights

- The Controller may audit the Processor's compliance with this DPA by providing **30 business days' written notice**.
- Audits are limited to **once per 12-month period**, unless a Data Breach or material non-compliance with this DPA has been identified, in which case additional audits may be conducted.
- The Processor shall cooperate with audits and provide reasonable access to relevant records, systems, and personnel.
- Audit costs shall be borne by the Controller, except where an audit reveals material non-compliance by the Processor, in which case the Processor shall bear the reasonable costs of the audit.

9. Data Breach Notification

- The Processor shall notify the Controller of any suspected or confirmed Data Breach **without undue delay and no later than 72 hours** after becoming aware of the breach.
- The notification shall include:
  - A description of the nature of the breach, including the categories and approximate number of individuals affected
  - The name and contact details of the Processor's point of contact
  - A description of the likely consequences of the breach
  - A description of the measures taken or proposed to address the breach, including measures to mitigate possible adverse effects
- The Processor shall cooperate with the Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of the Data Breach.
- The Processor shall assist the Controller in meeting its notification obligations under the **Notifiable Data Breaches (NDB) scheme** (Part IIIC of the Privacy Act 1988).

10. Cross-Border Data Transfers

Where personal information is transferred outside Australia (specifically to Anthropic in the United States for AI processing), the Processor ensures that:

- The transfer is necessary for the performance of the Services.
- The overseas recipient is bound by enforceable obligations that are substantially similar to the APPs.
- The Processor remains accountable under APP 8 for the overseas recipient's handling of personal information.
- All cross-border transfers use TLS-encrypted connections.
- Data transmitted to the AI provider is processed transiently and not permanently stored.

For full details of cross-border disclosure arrangements, see the Processor's Privacy Policy (v5.0), Section 8.

11. Term and Termination

11.1 Duration

This DPA commences on the effective date of the Service Agreement and remains in force until the Service Agreement is terminated or expires, and all personal information has been deleted or returned.

11.2 Post-Termination Data Handling

- Upon termination of the Service Agreement, the Processor shall, at the Controller's election, either return or securely delete all personal information within **30 days**.
- The Processor may retain personal information to the extent required by applicable law, in which case the Processor shall continue to protect the information in accordance with this DPA.
- The Processor shall provide written confirmation of deletion upon request.

11.3 Survival

Sections relating to confidentiality, data breach notification, audit rights, and liability shall survive termination of this DPA.

12. Contact

Salim Zakkour trading as OpsBots
ABN: 22 838 356 145

Contact Type	Details
DPA enquiries	hello@opsbots.com.au
Data breach reporting	hello@opsbots.com.au
Audit requests	hello@opsbots.com.au

This Data Processing Agreement should be read together with the Privacy Policy (v5.0) and Terms of Service (v2.2). It should be reviewed by a qualified Australian privacy lawyer before execution.