OpsBots Privacy Policy

Entity: Salim Zakkour trading as OpsBots **ABN:** 22 838 356 145 **Version:** 5.0

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

---

1. About This Policy (APP 1 — Open and Transparent Management)

Salim Zakkour trading as OpsBots (ABN 22 838 356 145) ("OpsBots", "we", "us", "our") is committed to protecting the privacy of personal information in accordance with the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**.

OpsBots is a sole trader business registered in Australia. References to "OpsBots" throughout this policy refer to the business operated by Salim Zakkour under ABN 22 838 356 145.

This Privacy Policy describes how we collect, hold, use, disclose, and otherwise manage personal information in connection with our AI-powered Managed Service Provider (MSP) support services.

This policy applies to:

- MSP clients who contract OpsBots services
- End-users whose data is processed through MSP client systems
- Visitors to our website (opsbots.com.au)
- Prospective clients and business contacts

This policy is freely available on our website and upon request. We review and update this policy at least annually or when our data practices materially change. Any updates will be published and communicated to affected parties.

Contact for privacy enquiries: hello@opsbots.com.au

2. Anonymity and Pseudonymity (APP 2)

Individuals have the option of not identifying themselves, or of using a pseudonym, when dealing with OpsBots — where it is lawful and practicable to do so.

Anonymity or pseudonymity may not be practicable in the following circumstances:

- When providing AI ticket classification services, as ticket data is linked to specific devices, users, or organisations
- When entering into a commercial agreement with OpsBots
- When OpsBots is required by law to verify identity

Where anonymity is not practicable, we will explain why identification is necessary.

3. Collection of Solicited Personal Information (APP 3)

We collect only personal information that is **reasonably necessary** for the provision of our MSP AI support services. The categories of personal information we may collect include:

3.1 MSP Client Personnel

- Contact details: name, email address, phone number, job title
- Account credentials: usernames, API keys (stored encrypted)
- Billing information: business name, ABN, billing address, payment details

3.2 End-User Data (via MSP Client Systems)

When our AI-powered systems process IT support tickets on behalf of MSP clients, the following categories of personal information may be present in ticket data:

- **Identifiers:** names, email addresses, employee IDs, usernames
- **Device information:** device names, IP addresses, MAC addresses, serial numbers
- **IT support content:** descriptions of technical issues, error messages, system logs
- **Potentially sensitive information:** depending on the MSP client's business, tickets may contain health information, financial details, or other sensitive categories

Important: OpsBots does not independently collect end-user personal information. End-user data enters our systems only through the MSP client's Professional Services Automation (PSA) integration. The MSP client remains the primary data controller for their end-user data.

3.3 Website Visitors

- Standard web analytics: IP address, browser type, pages visited
- Contact form submissions: name, email, message content

3.4 What We Do NOT Collect

- We do not collect personal information beyond what is reasonably necessary
- We do not use client data to train AI models
- We do not harvest or aggregate personal information across MSP clients
- We do not collect Tax File Numbers, government identifiers, or biometric data

4. Dealing with Unsolicited Personal Information (APP 4)

If OpsBots receives personal information that was not solicited (e.g., personal details included in support tickets that are not relevant to the service request), we will:

1. **Assess** whether we could have collected it under APP 3 (i.e., whether the information is reasonably necessary for our functions or activities)

2. **Retain** the information if collection would have been permitted under APP 3, and handle it in accordance with the APPs
3. **Destroy or de-identify** the information as soon as practicable if we determine we could not have collected it — unless retention is required by law

This assessment will be completed within **10 business days** of receiving the unsolicited information.

5. Notification of Collection (APP 5)

At or before the time of collection, we notify individuals (or, for end-user data, the MSP client for onward notification) about:

- The identity of the collecting entity (Salim Zakkour trading as OpsBots, ABN 22 838 356 145)
- The purposes of collection (AI-powered IT support processing)
- The types of entities to which information may be disclosed
- That this Privacy Policy contains information about access, correction, and complaints
- Whether collection is required by law or is voluntary
- The consequences of not providing the information

MSP clients are contractually required (via the Data Processing Agreement) to provide appropriate collection notices to their end-users before activating OpsBots services.

6. Use and Disclosure of Personal Information (APP 6)

We collect and use personal information for the following primary purposes:

Purpose	Description
Service delivery	Processing IT support tickets via AI-powered systems, including ticket classification, response generation, and escalation
Service management	Account administration, integration configuration, performance monitoring
Communication	Service notifications, support communications, incident alerts
Billing	Invoicing, payment processing, financial record-keeping
Service improvement	Analysing aggregate, de-identified service performance metrics
Compliance	Meeting legal and regulatory obligations, responding to lawful requests

We will not use personal information for a secondary purpose unless:

- The individual has consented, or
- The individual would reasonably expect us to use it for that purpose and it is related to the primary purpose, or
- It is required or authorised by law

We do not sell, rent, or trade personal information. We do not share personal information between MSP clients.

Disclosure Recipients

Recipient	Purpose	Safeguards
MSP client	Returning processed ticket data, reports, and AI-generated responses	Governed by service agreement and DPA

Recipient	Purpose	Safeguards
AI infrastructure provider (Anthropic)	Processing ticket content through AI models	See Section 8 (Cross-border disclosure)
Hosting infrastructure (self-hosted)	Primary data storage and processing	See Section 8.1 (Data residency)
Payment processors	Processing subscription payments	PCI-DSS compliant processors only
Professional advisors	Legal, accounting, or audit services	Bound by professional confidentiality
Law enforcement / regulators	As required by law, court order, or regulatory request	Only as legally compelled

7. Direct Marketing (APP 7)

OpsBots does not use personal information for direct marketing without consent.

- **No unsolicited marketing:** We will not use personal information collected through our ticket classification platform for direct marketing purposes without the individual's express consent
- **Product updates:** Where we send product updates or service communications to MSP client contacts, we will:
  - Always provide a clear and functional opt-out mechanism
  - Process opt-out requests within 5 business days
  - Never use sensitive information for direct marketing
  - Ensure the individual has a reasonable expectation of receiving such communications, or has consented
- **Third-party marketing:** We will never disclose personal information to third parties for their direct marketing purposes

8. Cross-Border Disclosure (APP 8)

8.1 Data Residency — Self-Hosted Australian Infrastructure

OpsBots's primary infrastructure is **self-hosted on dedicated hardware located in New South Wales, Australia**. This is privately owned and operated infrastructure — not a third-party cloud or IaaS provider. All persistent data storage — including task queues, documentation, and operational data — resides on this self-hosted Australian infrastructure.

Infrastructure details:

- **Type:** Self-hosted, privately owned server hardware
- **Location:** New South Wales, Australia
- **Operator:** OpsBots (Salim Zakkour)
- **Network:** Secured via private VPN (Tailscale) with no public internet exposure of management interfaces
- **No third-party hosting provider:** Data is not stored on AWS, Azure, Google Cloud, or any other cloud IaaS platform

Because the infrastructure is self-hosted and operated directly by OpsBots, there is no sub-processor relationship for data storage. OpsBots maintains full physical and logical control over all stored data.

8.2 AI API Processing — Overseas Disclosure

Our services use the **Anthropic Claude API** for AI-powered ticket classification and natural language processing. When tickets are processed via the Claude API, ticket content is transmitted to Anthropic's infrastructure in the **United States**. In this scenario:

- Data is transmitted via TLS-encrypted connections
- Anthropic does not retain prompt data for model training (confirmed under Anthropic's commercial terms)
- Processing is transient — data is not permanently stored by the AI provider

- OpsBots remains accountable under APP 8 for ensuring the overseas recipient handles data in accordance with the APPs

Recipient	Country	Purpose	Data Retained?
Anthropic (Claude API)	United States	AI-powered ticket classification and natural language processing	No — transient processing only

8.3 Data Sovereignty Options

MSP clients with strict data sovereignty requirements (e.g., government, financial services under APRA CPS 234) will be flagged for review before service activation. We will work with such clients to configure services that meet their residency requirements, which may include limiting or excluding AI API processing for their data.

9. Government-Related Identifiers (APP 9)

OpsBots does not adopt government-related identifiers (such as Tax File Numbers, Medicare numbers, ABN/ACN, driver's licence numbers, or passport numbers) as its own identifiers for individuals.

We will not collect, use, or disclose government-related identifiers unless:

- It is required or authorised by Australian law or a court/tribunal order
- It is reasonably necessary for identity verification purposes in connection with our services, and only with the individual's consent
- It falls within a prescribed exception under the Privacy Regulations

Where government identifiers are inadvertently received (e.g., included in support ticket content), they will be handled under our APP 4 unsolicited information procedures and destroyed or de-identified as soon as practicable.

10. Quality of Personal Information (APP 10)

OpsBots takes reasonable steps to ensure that the personal information we collect, use, and disclose is accurate, up-to-date, complete, and relevant.

We maintain data quality through:

- Regular review of client contact information during contract renewal cycles
- Automated data validation checks on ticket submissions
- Providing individuals with the ability to update their own information (see Section 14)
- Periodic audits of stored personal information to identify and correct inaccuracies

11. Security of Personal Information (APP 11)

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure.

11.1 Technical Controls

- **Encryption in transit:** All data transmitted via TLS 1.2+
- **Encryption at rest:** API keys and credentials stored in encrypted vaults; disk encryption on server hardware
- **Access control:** Role-based access with tiered authority levels
- **Network security:** Private network (Tailscale VPN) for inter-service communications; no public internet exposure of management interfaces
- **Authentication:** SSH key-based access; MFA for administrative functions
- **Monitoring:** Automated fleet health monitoring and anomaly detection

11.2 Operational Controls

- **Data isolation:** Strict separation of data between MSP clients — no cross-client data access
- **Least privilege:** Systems and operators operate with minimum necessary permissions

- **Audit logging:** All system actions logged with timestamps for accountability
- **Incident response:** Documented data breach response procedures (see Section 17)

11.3 Data Retention and Destruction

- Ticket data processed by AI is ephemeral — content is not retained after classification
- Client data is retained for the duration of the service agreement plus any legally required retention period
- Upon contract termination, client data is securely deleted within 30 days unless legal obligations require longer retention
- We destroy or de-identify personal information when it is no longer needed for any purpose permitted under the APPs

12. Access to Personal Information (APP 12)

Individuals have the right to request access to personal information that OpsBots holds about them.

- **How to request:** Email hello@opsbots.com.au with the subject line "Privacy Access Request"
- **Verification:** We will verify your identity before providing access
- **Response timeframe:** Within **30 days** of receiving the request
- **Format:** We will provide access in the manner requested where reasonable and practicable (e.g., electronic copy, inspection)
- **Fees:** We may charge a reasonable fee where the request requires significant effort. We will inform you of any fee before proceeding
- **Refusal:** We may refuse access in limited circumstances permitted by the Privacy Act (e.g., where access would pose a serious threat to life or safety, or would unreasonably impact the privacy of other individuals). Where we refuse, we will provide written reasons and information about complaint options

13. Correction of Personal Information (APP 13)

If an individual believes that personal information held by OpsBots is inaccurate, out-of-date, incomplete, irrelevant, or misleading, they may request correction:

- **How to request:** Email hello@opsbots.com.au with the subject line "Privacy Correction Request"
- **Response timeframe:** Within **30 days**
- **Refusal:** If we decline to correct, we will provide written reasons and, at the individual's request, associate a statement noting the individual's view that the information is inaccurate or incomplete
- **Notification:** Where we correct information previously disclosed to a third party, we will take reasonable steps to notify that third party

14. Your Rights

In addition to the access and correction rights described above, you have the following rights under the Privacy Act 1988 and the Privacy and Other Legislation Amendment Act 2024:

14.1 Right to Erasure

You may request that we delete your personal information. We will comply unless we are required by law to retain the information, or the information is necessary for an ongoing service agreement. Erasure requests will be actioned within **30 days**.

Upon erasure, we will:

- Delete or de-identify all personal information we hold about you
- Notify any third parties to whom we have disclosed your information to also delete it where practicable
- Confirm completion of erasure in writing

14.2 Right to Object

You may object to the processing of your personal information for a particular purpose. Where you object, we will cease processing for that purpose unless we have a lawful basis to continue (e.g., legal obligation or legitimate interest that overrides your objection).

To object, contact hello@opsbots.com.au with the subject line "Privacy Objection". We will acknowledge your objection within **5 business days** and provide a substantive response within **30 days**, including our decision and reasoning.

14.3 Right to Data Portability

You may request a copy of your personal information in a structured, commonly used, machine-readable format. We will provide portable data within **30 days** of your request.

Available export formats:

- CSV (Comma-Separated Values)
- JSON (JavaScript Object Notation)

Portable data will include all personal information we hold about you in a format that allows you to transfer it to another service provider.

14.4 How to Exercise Your Rights

To exercise any of these rights, contact us at **hello@opsbots.com.au** with the subject line "Privacy Rights Request". We will:

1. Acknowledge your request within **5 business days**
2. Verify your identity
3. Respond substantively within **30 days**
4. Provide written reasons if we cannot fully comply with your request

15. AI Disclosure and Automated Decision-Making

OpsBots uses **artificial intelligence (AI)** — specifically **Anthropic's Claude**, a large language model — as a core component of our service delivery. In accordance with the Privacy Act 1988, the Privacy and Other Legislation Amendment Act 2024, and Australia's National AI Plan (December 2025), we are committed to full transparency about how AI is used in our operations.

15.1 How We Use AI

AI Function	Description	Human Oversight
Ticket classification	AI categorises and prioritises IT support tickets submitted by MSP clients	Results reviewed by MSP support staff
Response generation	AI generates suggested responses for support staff review	All responses subject to human approval before sending to end-users
Pattern detection	AI identifies trends and recurring issues across ticket data	Reports reviewed by operations team
Escalation recommendations	AI flags tickets requiring urgent human attention	Human decision on all escalations
Internal operations	AI assists with internal task management, documentation, and operational workflows	Supervised by OpsBots operations team

15.2 Automated Decision-Making (ADM)

In compliance with the automated decision-making disclosure requirements effective **10 December 2026** (Privacy and Other Legislation Amendment Act 2024), OpsBots discloses the following:

- **AI ticket classification** constitutes automated decision-making that may affect the priority and routing of support requests. These decisions influence response times but do not deny service or access to any individual.

- **No fully automated decisions** with significant legal or similarly significant effects are made without human review.
- Individuals may request **human review** of any AI-generated classification or recommendation by contacting their MSP provider or hello@opsbots.com.au.
- Individuals have the right to receive a **meaningful explanation** of how an automated decision was reached, including the key factors and logic involved in the AI's classification or recommendation. To request an explanation, contact hello@opsbots.com.au with the subject line "ADM Explanation Request".

15.3 AI Data Handling

- Client ticket data sent to the AI provider (Anthropic) is **not used for model training** under Anthropic's commercial terms
- AI processing of ticket content is **transient** — data is not permanently stored by the AI provider after processing
- Personal information within tickets is processed only for the **primary purpose** of ticket classification and response generation
- We do not use personal information to build profiles, score individuals, or make predictions about individuals beyond the scope of the specific support request

15.4 AI Safeguards

- AI-generated outputs are subject to human review controls as defined in each service agreement
- OpsBots's AI systems identify themselves as AI in all end-user interactions — they **never impersonate humans**
- We maintain oversight of AI system behaviour through **audit logging and monitoring**
- We regularly review AI outputs for **accuracy, bias, and appropriateness**
- Clients may request information about how AI has processed their data at any time

16. Consent Mechanisms

16.1 How We Obtain Consent

Consent Type	When Used	Mechanism
Contractual consent	MSP client onboarding	Execution of the Service Agreement and Data Processing Agreement (DPA), which includes explicit consent to AI-powered ticket processing
Informed consent	Before AI processing of end-user data	MSP clients are contractually required to inform their end-users that AI-powered systems (including Anthropic's Claude) will process support ticket data, and to obtain any necessary consents
Collection notice consent	At point of data collection	Collection notices presented during onboarding, within platform interfaces, and via API documentation clearly state what data is collected and how it is used
Marketing consent	Before any marketing communications	Opt-in consent obtained separately; not bundled with service consent

16.2 What You Are Consenting To

By using OpsBots's services (directly or through your MSP provider), you consent to the following:

- Collection and processing of personal information contained in IT support tickets
- Use of AI (Anthropic's Claude) for ticket classification, response generation, and pattern analysis
- Transient cross-border transmission of ticket data to Anthropic's infrastructure in the United States for AI processing (see Section 8)
- Retention of personal information for the duration of the service agreement plus any legally required retention period

16.3 Withdrawing Consent

You have the right to withdraw consent at any time. To withdraw consent:

- **MSP clients:** Provide written notice to hello@opsbots.com.au. Withdrawal of consent for core AI processing will result in suspension of AI-powered services, as AI processing is integral to service delivery. Non-essential processing (e.g., marketing, analytics) can be withdrawn without affecting core service.
- **End-users:** Contact your MSP provider to request that your data not be processed by OpsBots's AI systems, or contact us directly at hello@opsbots.com.au. We will work with your MSP provider to accommodate your request where practicable.

Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

16.4 Consent for Sensitive Information

Where support tickets contain **sensitive information** (as defined under the Privacy Act 1988 — including health information, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, or criminal records), OpsBots processes this data only with the individual's consent or where required by law. MSP clients operating in sensitive sectors (e.g., healthcare, legal, financial) must ensure appropriate consents are in place before activating OpsBots services.

16.5 Children's Data

OpsBots does not knowingly collect personal information from individuals under the age of 18. If we become aware that we have collected personal information from a child without verified parental consent, we will take steps to delete that information promptly.

17. Notifiable Data Breaches (NDB Scheme)

Under Part IIIC of the Privacy Act 1988, OpsBots is subject to the **Notifiable Data Breaches (NDB) scheme**. A data breach is notifiable when there is unauthorised

access to, disclosure of, or loss of personal information that is likely to result in serious harm.

Our Response Procedure

1. **Contain** the breach immediately — isolate affected systems, revoke compromised credentials
2. **Assess** within 30 days — determine the type of information involved, number of individuals affected, and whether serious harm is likely
3. **Notify** if required — notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable
4. **Remediate** — implement measures to prevent recurrence, including root cause analysis
5. **Record** — maintain a register of all data breaches for internal review

Report a suspected breach: hello@opsbots.com.au

18. Statutory Tort for Serious Privacy Invasions

OpsBots acknowledges the statutory tort for serious invasions of privacy introduced by the **Privacy and Other Legislation Amendment Act 2024**. This provision creates a legal cause of action for individuals who suffer a serious invasion of their privacy.

OpsBots is committed to handling all personal information in a manner that respects individual privacy and minimises the risk of any privacy invasion. Our data handling practices, security measures, and consent mechanisms described in this policy are designed to ensure that personal information is treated lawfully and responsibly.

If you believe your privacy has been seriously invaded in connection with OpsBots's services, you may:

1. Lodge a complaint with OpsBots (see Section 19)
2. Lodge a complaint with the Office of the Australian Information Commissioner (OAIC)

3. Seek legal advice regarding your rights under the statutory tort provisions

19. Complaints

If you believe we have breached the Australian Privacy Principles or handled your personal information inappropriately, you may lodge a complaint:

1. **Contact us first:** Email hello@opsbots.com.au with the subject line "Privacy Complaint". We will acknowledge your complaint within **5 business days** and respond within **30 days**.
2. **External complaint:** If you are unsatisfied with our response, you may lodge a complaint with the **Office of the Australian Information Commissioner (OAIC)** at www.oaic.gov.au or by calling **1300 363 992**.

20. Contact Details

Salim Zakkour trading as OpsBots
ABN: 22 838 356 145

Contact Type	Details
Privacy enquiries	hello@opsbots.com.au
Complaints	hello@opsbots.com.au (subject: "Privacy Complaint")
Access/correction requests	hello@opsbots.com.au
AI processing enquiries	hello@opsbots.com.au
Data breach reporting	hello@opsbots.com.au

Contact Type	Details
ADM explanation requests	hello@opsbots.com.au (subject: "ADM Explanation Request")
Rights requests (erasure, objection, portability)	hello@opsbots.com.au (subject: "Privacy Rights Request")

21. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, or legal requirements. We will:

- Publish the updated policy on our website
- Notify MSP clients of material changes via email
- Note the effective date and version number of each update

APP Coverage Summary

APP	Principle	Section
APP 1	Open and transparent management	Section 1
APP 2	Anonymity and pseudonymity	Section 2
APP 3	Collection of solicited personal information	Section 3
APP 4	Dealing with unsolicited personal information	Section 4
APP 5	Notification of collection	Section 5

APP	Principle	Section
APP 6	Use or disclosure of personal information	Section 6
APP 7	Direct marketing	Section 7
APP 8	Cross-border disclosure	Section 8
APP 9	Government-related identifiers	Section 9
APP 10	Quality of personal information	Section 10
APP 11	Security of personal information	Section 11
APP 12	Access to personal information	Section 12
APP 13	Correction of personal information	Section 13
—	Individual Rights (erasure, objection, portability)	Section 14
—	AI Disclosure and Automated Decision-Making	Section 15
—	Consent Mechanisms	Section 16
—	Notifiable Data Breaches	Section 17
—	Statutory Tort Acknowledgment	Section 18

This Privacy Policy has been prepared in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles, and the Privacy and Other Legislation Amendment

Act 2024. It should be reviewed by a qualified Australian privacy lawyer before external publication.