

PRIVACY POLICY

Effective Date: 12 March 2026

Entity: AARON THOMAS PARTON (ABN 30 520 399 153),

trading as Mycelium AI

Contact: aaron@myceliumai.com.au

1. Who We Are

This Privacy Policy explains how AARON THOMAS PARTON (ABN 30 520 399 153), trading as Mycelium AI ("Mycelium AI", "we", "us", "our"), collects, uses, discloses, and protects personal information in connection with our AI and automation consulting, web development, and systems implementation services.

Contact (privacy): aaron@myceliumai.com.au

We primarily serve businesses in Australia but may provide services globally.

2. Scope

This Policy applies to personal information processed via:

- Our website at www.myceliumai.com.au (and any client websites we host or manage).
- Our forms, webhooks, and integrations (e.g., Calendly, Stripe, Google Workspace/Sheets/Drive, n8n flows, Cloudflare, Netlify, Vercel, GoDaddy, Power BI, Momence, and similar tools used in service delivery).
- Our service delivery activities (including data we process on behalf of our clients).

3. What We Collect

We collect the following categories of personal information:

Business/contact data: Name, role/title, company name and details, email, phone, budget and project information. Domain registration details (registrant name, contact information) collected for domain management services.

Service credentials and technical data (highly confidential): API keys, usernames, passwords, connection tokens, system configuration details, logs, and related technical artifacts provided by clients for integration purposes.

Client end-user data: Where required to deliver services (e.g., data from a client's CRM, form responses, transactions, or other system records) we may process client end-users' personal information as a processor on the client's instructions.

Financial/transaction data: Billing contact details and transaction references. Card payments are processed by third-party gateways (e.g., Stripe); we do not store full card numbers.

Automatically collected data: Basic device/usage data and cookies/analytics (see Cookies & Analytics section).

We do not intentionally collect sensitive information about individuals (e.g., health, biometrics) unless it is strictly necessary for a stated purpose and provided by or on behalf of the client.

4. How We Collect Information

- Directly from you (forms, emails, calls, uploads).

- Through connectors/APIs and automation platforms (e.g., n8n, Google/Microsoft apps, CRMs) when you authorise integrations.
- From our clients in order to provide services to them (acting as a processor).
- Limited automatic collection via cookies and analytics.

5. Why We Use Information (Purposes)

We use personal information to:

- Respond to enquiries, assess opportunities, and scope projects.
- Deliver, operate, and maintain automations, integrations, websites, and related services.
- Register, configure, and manage domains on your behalf.
- Set up and manage website hosting, DNS, and SSL certificates.
- Configure and manage paid advertising campaigns (Google Ads, Meta Ads) on your behalf.
- Secure our systems and yours (access controls, logging, abuse prevention).
- Manage accounts, invoicing, and payments.
- Conduct analytics (service performance, site usage) and improve our offerings.
- Send service communications, and (where permitted) direct marketing with an unsubscribe option.
- Comply with laws and enforce our agreements.

AI/Model use and improvement:

- We may send personal or business data to AI vendors (e.g., OpenAI, Anthropic, Google, AWS Bedrock/Microsoft) only as needed to deliver the requested functionality.
- We do not permit third-party foundation model providers to train their models on your data by default.
- For our internal improvement, we may use anonymised or aggregated data (stripped of direct identifiers) to refine prompts, templates, and tools. You may opt out by contacting us.

We will not use client-provided personal information for our own unrelated marketing.

6. Our Role: Controller vs. Processor

Controller (our own business data): We act as a controller for data we collect about prospects, clients, and visitors (e.g., contact details).

Processor (client end-user data): We act as a processor when handling client end-user data under the client's written instructions. The client is responsible for having a lawful basis and providing any required notices to its end-users.

7. Legal Bases (EU/UK Visitors)

Where applicable (e.g., EU/UK), we rely on: performance of a contract, legitimate interests (e.g., service operation, security), consent (for cookies/marketing where required), and legal obligations.

8. Disclosures to Third Parties

We may share personal information with:

- Service providers / subprocessors: e.g., cloud hosting, analytics, productivity suites (Google/Microsoft), automation platforms (n8n), payment processors (Stripe), scheduling (Calendly), CRMs, ticketing, and communications tools.
- Domain registrars (e.g., GoDaddy, Cloudflare) to register and manage domains on your behalf.
- Hosting providers (e.g., Netlify, Vercel, Cloudflare Pages) to host and deploy websites.
- Advertising platforms (e.g., Google Ads, Meta/Facebook Ads) to configure and manage paid advertising campaigns on your behalf.
- SEO and analytics tools (e.g., Google Analytics, Google Search Console) to monitor website performance.
- Contractors/subcontractors: bound by confidentiality and data-processing terms, with restricted, role-based access limited to necessity.
- Professional advisers (legal, accounting) and authorities where legally required.
- Business transfers (e.g., restructuring).

We do not "sell" personal information.

9. International Transfers

We primarily operate in Australia but may transfer personal information to providers or authorised personnel in other countries. Where we do, we use reasonable safeguards (contractual protections, reputable vendors, encryption in transit/at rest where applicable).

10. Security

We use administrative, technical, and organisational measures appropriate to the risk, including:

- Role-based access control and least-privilege; access reviews.
- Multi-factor authentication and SSO where supported.
- Encryption in transit (TLS) and at rest where supported by vendors.
- Secrets management (vaulting) for API keys and credentials; redaction from logs; credential rotation on request or at project end.
- Prohibition on sending passwords/API keys over email or unsecured chat; use of secure channels.
- Internal policies for device security, change control, and incident response.

No system is perfectly secure; we cannot guarantee absolute security.

11. Retention & Deletion

We keep personal information only as long as necessary for the purposes above or as required by law. Unless agreed otherwise with a client:

- Enquiry/sales records: up to 24 months after last interaction.
- Project files & operational logs: generally up to 7 years after project close.
- Service credentials: deleted within 90 days of termination/hand-over.

- Prompt/output QA logs: typically up to 180 days.
- Analytics data: up to 26 months.

Clients may request data return or destruction at project close; we will action within a reasonable period, subject to legal holds.

12. Your Choices & Rights

Subject to applicable law, you may request access, correction, deletion, or a copy of your personal information, or object/restrict certain processing.

How to make a request: email aaron@myceliumai.com.au. We may need to verify your identity and will respond within a reasonable timeframe (or one month where GDPR applies).

You can opt out of marketing at any time via unsubscribe instructions in our emails or by contacting us.

13. Cookies & Analytics

We may use cookies/SDKs and similar technologies for site functionality, analytics, and (where enabled) remarketing.

- We will display a cookie notice and, where required, obtain consent.
- We will endeavour to honour supported browser Global Privacy Control/Do Not Track signals where feasible.
- You can manage cookies via your browser settings; disabling some cookies may affect site functionality.

Details of specific tools (e.g., GA4, Meta, LinkedIn, or others) will be listed in our cookie notice and updated as our stack evolves.

14. Children

Our services are for business users. We do not knowingly collect personal information from children under 16.

15. Data Breaches (Australia's NDB Scheme)

If a data breach is likely to result in serious harm, we will assess promptly and, where required by law, notify affected individuals and the Office of the Australian Information Commissioner (OAIC).

16. Third-Party Links

Our website and documents may link to third-party sites or services. Their privacy practices are governed by their own policies.

17. Changes to This Policy

We may update this Policy from time to time. The "Effective date" shows the latest version. Material changes will be announced via our website or by email where appropriate.

18. Contact

Questions, requests, or complaints (including escalation if unresolved): aaron@myceliumai.com.au.

Unresolved privacy complaints in Australia can be lodged with the OAIC.