



AI Automation & Custom Software

aias.co.nz | info@aias.co.nz

Privacy Policy

Last updated: 5 June 2026

Company	AIAS Digital
Country	New Zealand
Website	aias.co.nz
Privacy Contact	info@aias.co.nz
Last Updated	5 June 2026

Important: This policy has been prepared for AIAS Digital. It should be reviewed by a qualified lawyer before publication, especially if you process health, financial, insurance, employment, biometric, children's, or other high-risk data.

This Privacy Policy explains how AIAS Digital collects, uses, stores, discloses, transfers, and protects personal information when you visit our website, contact us, use our services, interact with our AI tools, or otherwise provide information to us.

We are based in New Zealand and provide AI automation, workflow automation, AI agents, chatbots, CRM integrations, data processing, marketing automation, business process automation, and related technology services.

For the purposes of this Privacy Policy:

- "we", "us", or "our" means AIAS Digital.
- "you" or "your" means website visitors, prospective clients, clients, client staff, end users, suppliers, contractors, and any person whose personal information we process.
- "personal information" means information about an identifiable individual.
- "client data" means information provided to us by or on behalf of our clients.
- "AI services" means services involving artificial intelligence, machine learning, large language models, automation tools, AI agents, chatbots, or similar technologies.

1. Who We Are

- Business name: AIAS Digital
- Country: New Zealand
- Website: aias.co.nz
- Privacy contact: info@aias.co.nz

2. Scope of This Privacy Policy

This Privacy Policy applies to personal information we collect through:

- our website
- contact forms, booking forms, enquiry forms, email, phone, SMS, or social media
- sales, onboarding, support, and client communications

- AI automation projects and workflow builds
- chatbots, AI agents, forms, dashboards, integrations, and automation systems we provide
- analytics, cookies, pixels, and similar tracking technologies
- events, demos, proposals, contracts, invoices, and business dealings
- recruitment, contractor, and supplier interactions

3. Personal Information We Collect

We only collect personal information that is reasonably necessary for our business, our services, legal compliance, security, or another lawful purpose.

3.1 Contact and Identity Information

- full name
- business name
- job title
- email address
- phone number
- address or region
- social media profile or LinkedIn URL
- website URL
- communication preferences

3.2 Business and Client Information

- company information
- business processes and workflows
- operational data
- CRM data
- sales, support, or customer service information
- project requirements
- documents, files, spreadsheets, forms, and records you provide
- proposal, contract, and billing information

3.3 AI, Automation, and Workflow Data

When we build, test, maintain, or operate AI automations, we may process:

- prompts and instructions
- chatbot messages
- AI agent conversations
- form submissions
- email content
- calendar data
- CRM records
- workflow logs
- automation outputs
- metadata
- model inputs and outputs

3.4 Website and Usage Information

- IP address
- device type
- browser type

- operating system
- pages viewed
- links clicked
- time spent on pages
- referring website
- approximate location
- cookie identifiers
- analytics identifiers

3.5 Payment and Billing Information

- billing name
- billing address
- invoice details
- payment status
- transaction records
- tax information

We do not usually store full card details. Payments may be processed by third-party payment providers.

3.6 Sensitive Information

We do not intentionally collect sensitive information unless it is necessary for a specific service, you provide it voluntarily, or our client instructs us to process it. Where required by law, we will obtain consent before processing sensitive information.

3.7 Children's Information

Our services are designed for businesses and are not directed at children. We do not knowingly collect personal information from children without appropriate consent.

4. How We Collect Personal Information

We may collect personal information:

- directly from you
- from our clients
- from forms, emails, calls, meetings, or documents
- through our website and online tools
- through software integrations
- from public sources such as company websites, LinkedIn, or business directories
- automatically through cookies and similar technologies

5. Why We Use Personal Information

5.1 To Provide Our Services

- building AI automations
- creating workflows
- integrating software systems
- developing chatbots or AI agents
- testing, troubleshooting, and improving automations
- providing support and maintenance
- managing projects and deliverables

5.2 To Communicate with You

- responding to enquiries

- booking meetings
- sending proposals
- providing customer support
- managing client relationships

5.3 To Operate and Improve Our Business

- internal administration
- record keeping
- service improvement
- analytics
- quality assurance
- performance monitoring

5.4 To Operate and Improve AI Systems

- testing AI workflows
- monitoring output quality
- reducing errors
- improving accuracy
- detecting misuse
- evaluating system performance

Unless clearly stated in a client agreement or consented to by you, we do not use confidential client data to train publicly available AI models.

5.5 Marketing and Business Development

We may use personal information to send newsletters, service updates, educational content, and follow up on enquiries. You can unsubscribe from marketing communications at any time.

5.6 Security, Fraud Prevention, and Legal Compliance

- protect our systems
- prevent fraud, spam, abuse, or security incidents
- comply with legal obligations
- respond to lawful requests
- manage disputes

6. Legal Bases for Processing

Depending on your location and the circumstances, we may rely on:

- your consent
- performance of a contract
- our legitimate business interests
- compliance with legal obligations
- protection of vital interests
- another lawful basis available under relevant law

7. AI-Specific Privacy Terms

7.1 Use of AI Tools

We may use AI tools, large language models, machine learning systems, automation platforms, and third-party AI providers to deliver services.

7.2 AI Outputs

AI-generated outputs may be incomplete, inaccurate, outdated, or inappropriate. We recommend human review before relying on AI outputs, especially where they may affect legal rights, financial outcomes, or other important decisions.

7.3 No Solely Automated High-Impact Decisions Unless Agreed

Unless expressly agreed in writing, our services are not intended to make solely automated decisions that produce legal, financial, employment, or similarly significant effects on individuals.

7.4 Client Responsibility for AI Inputs

Clients are responsible for ensuring they have the right to provide personal information to us and to any connected AI or automation system.

7.5 Confidential Information and AI Model Training

We do not intentionally allow confidential client data to be used to train third-party public AI models without express client authorisation.

7.6 AI Monitoring and Safety

We may monitor AI system usage to prevent misuse, detect security issues, improve reliability, manage hallucination risk, and comply with law.

8. Client Data and Processor Role

When we process personal information on behalf of a client, we usually act as a service provider or processor. In that situation, we process the data only as directed by the client and in accordance with our written agreement.

9. Cookies and Tracking

We may use cookies and similar technologies on our website. These may include essential cookies, functional cookies, analytics cookies, and advertising cookies.

You can manage cookies through your browser settings. Some website features may not work properly if cookies are disabled.

10. Analytics and Advertising

We may use third-party analytics and advertising providers such as Google Analytics, Meta, LinkedIn, or similar platforms.

You may be able to opt out through your browser settings, platform-level privacy settings, or advertising preference tools.

11. When We Disclose Personal Information

We may disclose personal information to:

- our staff, contractors, and authorised personnel
- cloud hosting providers
- AI service providers
- automation platforms
- payment processors
- accountants, lawyers, insurers, and professional advisers
- analytics and advertising providers
- regulators, courts, law enforcement, or government agencies where required by law
- buyers or advisers in connection with a merger, acquisition, or sale of business assets

We only disclose personal information where we have a lawful reason and appropriate safeguards.

12. Third-Party Platforms and Integrations

Our services may integrate with third-party platforms including Gmail, Outlook, Google Workspace, Microsoft 365, Slack, HubSpot, Xero, Stripe, Zapier, Make, n8n, OpenAI, Anthropic, AWS, Supabase, and other client-selected platforms.

The privacy practices of third-party platforms are governed by their own terms and privacy policies.

13. International Transfers

We are based in New Zealand, but we may process, store, access, or transfer personal information in other countries where our service providers, cloud providers, AI providers, or clients are located.

Where required, we use appropriate safeguards for international transfers such as contractual protections, data processing agreements, and standard contractual clauses.

14. Security

We take reasonable technical, organisational, and administrative steps to protect personal information from loss, unauthorised access, misuse, disclosure, alteration, or destruction.

Security measures include access controls, multi-factor authentication, encryption in transit, encryption at rest, secure cloud infrastructure, and incident response procedures.

15. Data Retention

We keep personal information only for as long as reasonably necessary for the purposes described in this Privacy Policy, unless a longer period is required by law.

When information is no longer needed, we will take reasonable steps to delete, de-identify, anonymise, or securely archive it.

16. De-Identified, Anonymised, and Aggregated Data

We may use de-identified, anonymised, or aggregated information for analytics, service improvement, AI system evaluation, security monitoring, and business planning.

17. Your Privacy Rights

Depending on where you live, you may have rights to:

- request access to your personal information
- request correction of inaccurate information
- request deletion of your information
- object to processing
- restrict processing
- withdraw consent
- request data portability
- opt out of marketing
- complain to a privacy regulator

To exercise your rights, contact us at info@aias.co.nz.

18. New Zealand Privacy Rights

If you are in New Zealand, you have rights under the Privacy Act 2020, including the right to request access to and correction of your personal information.

You may also complain to the New Zealand Office of the Privacy Commissioner if you are not satisfied with our response.

19. European Union and United Kingdom Privacy Rights

If the EU GDPR or UK GDPR applies, you may have additional rights including the right to access, correct, erase, restrict, or port your personal data, and to lodge a complaint with a supervisory authority.

20. Australian Privacy Rights

If the Australian Privacy Act applies, you may have rights to access and correct personal information we hold about you. You may also complain to the Office of the Australian Information Commissioner.

21. Canadian Privacy Rights

If Canadian privacy law applies, you may have rights to know why your personal information is collected, access your personal information, request correction, and withdraw consent subject to legal or contractual restrictions.

22. California and US State Privacy Rights

If California or similar US state privacy laws apply, you may have rights to know what personal information we collect, request deletion or correction, opt out of sale or sharing, and not be discriminated against for exercising your rights.

23. Direct Marketing

We may send you marketing communications if you have consented, you are an existing client, or we have another lawful basis. You can unsubscribe at any time by clicking the unsubscribe link or contacting us.

24. Data Breach Notification

If we become aware of a privacy or security breach, we will take reasonable steps to contain, assess, and remediate it. Where required by law, we will notify affected individuals, clients, regulators, or other relevant parties.

25. Confidentiality

We treat client information, business information, workflow documentation, system architecture, prompts, automation logic, and related project materials as confidential unless otherwise agreed.

26. Client Obligations

Clients using our services must ensure that:

- they have a lawful basis to collect and provide personal information to us
- their own privacy policies and notices are accurate
- they have obtained all required consents
- they comply with employment, consumer, privacy, marketing, spam, AI, and industry-specific laws
- they review AI outputs before relying on them

27. Prohibited Uses

You must not use our services to:

- unlawfully collect, scrape, or process personal information
- send spam or unlawful marketing
- make unlawful automated decisions
- process sensitive information without authority
- generate harmful, misleading, or deceptive outputs
- violate any applicable law

28. High-Risk Use Cases

Some use cases involve higher privacy, fairness, and compliance risk. We may refuse, limit, or require additional safeguards for projects involving employment decisions, insurance eligibility, lending or financial decisions, health advice, biometric identification, or decisions affecting access to essential services.

29. Links to Other Websites

Our website may contain links to third-party websites. We are not responsible for the privacy practices, content, or security of third-party websites. You should review the privacy policies of any third-party websites you visit.

30. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The updated version will be posted on our website with a new "Last updated" date. Your continued use of our website or services after an update means you accept the updated Privacy Policy.

31. How to Contact Us

For privacy questions, requests, or complaints, contact:

- Email: info@aias.co.nz
- Website: aias.co.nz

We will take privacy complaints seriously and respond within a reasonable timeframe. If you are not satisfied with our response, you may contact your local privacy regulator.

© 2026 AIAS Digital. All rights reserved. | aias.co.nz | info@aias.co.nz