

Subprocessor & Hosting Register

DOCUMENT ID ATX-SOC-07	TITLE Subprocessor & Hosting Register
VERSION 1.0	CLASSIFICATION Public
OWNER Security Officer	APPROVED BY Chief Executive Officer
EFFECTIVE DATE 10 August 2026	NEXT REVIEW August 2027
STANDARDS MAPPING ISO/IEC 27001:2022 Annex A 5.19, 5.20, 5.21, 5.22, 5.23; SOC 2 TSC CC9.2, CC2.3	

1. Purpose and status

Atlastix develops and delivers Atlas Automate, Atlastix Observability, Atlastix Device Intelligence, and product extensions, integrations and custom software solutions. Current delivery is generally in customer- or MSP-controlled cloud tenancies. Deployment-specific architecture, data flows, hosting, processing locations and retention are governed by configuration and applicable agreements.

This register discloses four things: **Part A** - approved processing by Atlastix and the known cloud or corporate tools relevant to that processing; **Part B** - the AI-provider modes that may apply by product or deployment; **Part C** - the shared-responsibility position for in-tenancy deployments; and **Part D** - the specific current Device Intelligence customer annex. It is maintained from supplier-management records under ATX-PPL-05 and ATX-PPL-07.

Supplier locations and assurance vary by contracted service, plan, tenant and configuration. Except where this register states a verified current deployment fact, a location or certification is not asserted. Customers should refer to the provider's assurance material and the applicable service configuration.

2. Part A - Where customer data processed by Atlastix lives

Atlastix may process customer-approved extracts or uploads for development, customisation, testing, delivery or support, or use temporary customer-tenancy access without transferring a copy. A product or custom solution may also use an ongoing integration or feed where its purpose, data scope, location, security, retention and customer terms are documented and approved. The applicable deployment and agreement determine which paths apply.

WHAT	WHERE	DATA	CONTROLS REFERENCE
Approved engagement-data processing	Deployment- and agreement-specific approved environment	Customer-approved extracts or uploads for development, customisation, testing, delivery or support. Data may include personal information or end-client data where necessary and approved. Credentials, tokens and secrets are excluded unless an approved design and secure process expressly require them.	ATX-ENG-05, ATX-ENG-06; ATX-SOC-03 section 5

WHAT	WHERE	DATA	CONTROLS REFERENCE
Temporary customer-tenancy access	Customer- or MSP-controlled tenancy	No copy need be transferred; access is named, scoped, logged, approved and controlled by the tenancy operator.	ATX-TEC-01, ATX-ENG-05
Business and support records	Applicable approved corporate tools listed below	Customer and prospect business contact details, contracts, engagement records and support correspondence. Raw customer datasets and secrets are not approved for corporate tools.	ATX-ENG-05, ATX-PPL-05, ATX-PPL-06

Processing location, retention and deletion follow the applicable product, deployment and agreement and are recorded under ATX-ENG-06. Part D states the specific location and 30-day post-engagement deletion lifecycle for the current Device Intelligence deployment.

The known cloud, engineering and corporate-tool relationships relevant to Atlastix operations are:

SUPPLIER	ROLE	CUSTOMER DATA PROCESSED	LOCATION	SUPPLIER ASSURANCE STATEMENT
Microsoft (Azure and Entra ID)	Azure hosts applicable Atlastix engineering or approved engagement-data processing; Entra ID provides personnel identity and access	Data depends on the approved Azure workload; personnel identity and access records are processed in Entra ID	Approved Device Intelligence engagement data: Azure Australia East (Part D). Other workloads follow the applicable tenant, region and service configuration	Assurance follows the contracted Microsoft service and configuration.
Amazon Web Services (AWS)	Cloud infrastructure used for applicable Atlastix development, build, delivery or corporate workloads	Data depends on the approved workload and configuration	Trust Centre access records: AWS Sydney (ap-southeast-2), via the Supabase managed database service below. Other workloads follow the applicable account, region and service configuration	Assurance follows the contracted AWS service and configuration.
GitHub	Source control and GitHub Actions CI/CD for products, customisations and custom software; release artifacts stored in GitHub Actions artifacts and GitHub Releases	Source code, release artifacts, change and workflow records, and engineering identities; raw customer datasets, uploads and credentials are excluded	GitHub.com cloud (hosted in the United States under standard plans)	Assurance follows the contracted GitHub service and plan.
Microsoft 365	Email, calendar, documents and business collaboration	Business correspondence, customer contact details and support correspondence; raw customer datasets and credentials are excluded	Follows the applicable Microsoft 365 tenant and service configuration	Assurance follows the contracted Microsoft 365 service and configuration.

SUPPLIER	ROLE	CUSTOMER DATA PROCESSED	LOCATION	SUPPLIER ASSURANCE STATEMENT
Slack	Team messaging	Incidental business contact or support context; raw customer datasets and credentials are excluded	Sydney data residency is electable for content data on eligible plans and excludes member-profile and membership data; the Atlastix election status is recorded in ATX-PPL-07 (verified 9 Aug 2026)	Assurance follows the contracted Slack service and plan.
Atlassian (Jira, Jira Service Management and Confluence)	Issue tracking, internal knowledge and support case management; support@atlastix.io creates Jira Service Management tickets	Customer contact details and engagement or support records; raw customer dataset contents and credentials are excluded	Sydney data residency is electable for product content data and excludes user-account and AI data; the Atlastix election status is recorded in ATX-PPL-07 (verified 9 Aug 2026)	Assurance follows the contracted Atlassian service and plan.
Vercel	Managed hosting service for the Atlastix marketing and trust websites	Public website content and ordinary hosting request metadata; website enquiry content is submitted through EmailJS	Global edge delivery; Trust Centre compute runs in Australia (Sydney region)	Assurance follows the contracted Vercel service and configuration.
Supabase	Managed Postgres database service storing Trust Centre access, undertaking and audit records	Access-request and sign-in records, confidentiality-undertaking acceptances, document view and download logs, rate-limiting records	Australia - AWS Sydney region (ap-southeast-2)	Assurance follows the contracted Supabase service and configuration.
EmailJS	Delivers website enquiry submissions and Trust Centre access-request notifications to the monitored Atlastix support mailbox	Enquirer business contact details and enquiry content	United States (US-only AWS hosting per the EmailJS privacy policy; verified 9 Aug 2026)	Assurance follows the contracted service and configuration.
Xero	Accounting, invoicing and payroll-related financial records	Personnel payroll-related information, company financial data and customer billing details; customer engagement datasets are excluded	United States (US cloud hosting per Xero's own subprocessor disclosure; verified 9 Aug 2026)	Assurance follows the contracted service and configuration.

SUPPLIER	ROLE	CUSTOMER DATA PROCESSED	LOCATION	SUPPLIER ASSURANCE STATEMENT
1Password Business	Approved credential vault for human-held work credentials and non-SSO secrets (ATX-TEC-02)	Stored work credentials and shared non-SSO secrets; where a customer or MSP provides a credential for approved customisation or support, it is stored only in 1Password Business or the ATX-TEC-03 secrets services	1Password Business account regions are the United States, Canada or the European Union (no Australian region); vault data is end-to-end encrypted under 1Password's published zero-knowledge model, and confirmation of the contracted account region is a recorded Atlastix control	Supplier review completed 9 August 2026 under ATX-PPL-05: SOC 2 Type II and ISO/IEC 27001:2022 (with 27017, 27018, 27701) verified via the 1Password Trust Center; data processing addendum with a 72-hour breach-notification commitment and a published subprocessor list.

Atlastix also operates an in-house CRM secured with Microsoft Entra SSO and encryption for sales and marketing contacts, consent status and suppression records. It is an internal system rather than a third-party supplier; any underlying approved hosting service remains governed through the supplier register.

The supplier used for approved engagement data depends on the product, deployment and agreement. Listing a provider does not mean it receives every customer's data or becomes a subprocessor for software operating in a customer-controlled tenancy. Part D identifies Microsoft Azure as the processor for the current Device Intelligence extract or upload path.

3. Part B - AI model providers

Atlastix currently operates no AI model-provider account receiving customer workflow content. Current product and custom-solution arrangements are customer-controlled, and the approved design and agreement determine account ownership, data path and processing location.

MODE	CURRENT POSITION	SUBPROCESSOR STATUS
Customer provider account and keys	The customer selects and contracts with the AI provider and controls its terms, configuration, keys and processing location.	Generally the customer's supplier rather than an Atlastix-managed subprocessor; the applicable agreement confirms responsibility.
Customer cloud-native model service	The service operates under the customer's cloud account and controls.	Part of the customer's supplier and tenancy arrangement rather than an Atlastix-managed subprocessor, unless the applicable agreement states otherwise.

An Atlastix-managed provider receiving customer workflow content is prohibited. It may be considered only after separate CEO approval, supplier/subprocessor, privacy and risk review, customer disclosure and approval, and an update to this register before any customer content flows.

Credentials, tokens and secrets must not be placed in prompts, extracts or support uploads unless an approved design and secure process expressly require them. Customer data supplied to Atlastix is not used by Atlastix to train AI models (ATX-ENG-07). Provider treatment follows the approved provider terms and configuration.

4. Part C - In-tenancy deployment and shared responsibility

Current Atlastix delivery is generally in customer- or MSP-controlled cloud tenancies. Production workloads and primary data generally remain under the tenancy operator's controls. The customer or MSP selects and contracts with its cloud provider and any customer-controlled AI provider; those providers are not Atlastix subprocessors merely because Atlastix software operates in that tenancy. Exact architecture, data flows and responsibility allocation follow the deployed configuration and agreement.

An approved engagement may use temporary in-tenancy access instead of transferring data. Such access is named, logged, scoped to the engagement, granted and revoked by the customer or MSP, and used by Atlastix only for the approved purpose. Temporary access does not make the customer, MSP or cloud provider an Atlastix subprocessor.

Customer-approved extracts or uploads and agreed integrations or feeds may transfer data to an approved Atlastix processor where the deployment and agreement define the purpose, scope, security, location and lifecycle.

5. Part D - Current Device Intelligence customer annex

The current Device Intelligence deployment is a staging instance inside the MSP's cloud tenancy, in user acceptance testing ahead of production. Workloads and data in that instance, including any end-client data, MSP operational data and connector credentials, remain there under the MSP's controls. There is no separate ongoing Device Intelligence product or telemetry feed to Atlastix for this deployment.

The approved Device Intelligence data paths to Atlastix are customer-approved point-in-time extracts or support uploads stored and processed in an access-restricted Atlastix Microsoft Azure environment in Australia East, or temporary access within the MSP tenancy. Raw extracts or uploads may include personal information or end-client data where approved, but credentials, tokens and secrets are excluded. Primary copies are deleted within 30 days after the engagement ends; storage-level replicated copies follow the primary and are deleted with it, and no separate backup copies are currently retained.

AI features for this Device Intelligence deployment use the customer's provider, account and keys, or a customer cloud-native model service. No Atlastix-managed AI provider is used and no workflow content is sent to one. The MSP's cloud provider and customer AI provider are selected and contracted by the customer or MSP and are not Atlastix-managed subprocessors.

6. How suppliers are governed

1. ATX-PPL-05 requires suppliers to be risk-tiered by service, data access and criticality; tiers are recorded in ATX-PPL-07.
2. The process requires security, confidentiality, data-protection, incident and exit terms to be reviewed proportionate to supplier risk.
3. Review of supplier assurance considers the contracted service, plan, region, tenant and configuration. Supplier certifications are not treated as Atlastix certifications or as assurance over customer-operated controls.
4. A supplier incident is handled under the Incident Response Plan and applicable legal and customer-agreement terms. Atlastix does not publish a universal supplier or customer notification period in this register.
5. Supplier exit includes revocation of integrations and credentials, retrieval or deletion of data as applicable, and updates to internal and public records.

Supplier assessment records and contractual details are controlled internal records.

7. Change notification

New or replaced subprocessors of customer data follow the notice and objection process, if any, in the applicable data-processing or customer agreement. This register is updated before an approved new Atlastix-managed subprocessor begins production processing. Material changes are assessed through supplier and risk-management processes.

Questions and update requests should be sent to support@atlastix.io. Any binding notification, objection or response timing is controlled by the applicable agreement.

8. Related documents

ATX-PPL-05 Supplier & Third-Party Risk Policy; ATX-PPL-07 Supplier Register (internal); ATX-ENG-05 Data Classification & Handling Policy; ATX-ENG-06 Data Retention & Disposal Policy; ATX-ENG-07 AI Governance & Responsible Use Policy; ATX-RES-01 Incident Response Plan; ATX-SOC-01 System Description; ATX-SOC-03 Atlastix Security Whitepaper; ATX-SOC-08 Security Terms & Control Position.

Revision history

VERSION	DATE	CHANGE	APPROVED BY
1.0	10 Aug 2026	Initial release	Chief Executive Officer