ASSETLAB CMMS SOFTWARE INC.

Incorporated under the laws of British Columbia, Canada

SUB-PROCESSOR LIST

Third-Party Service Providers Engaged to Process Customer Data

AssetLab CMMS Software Inc.

Classification	Public - published at https://assetlab.ca/trust
Version	1.9
Effective	12 October 2026
Prepared by	AssetLab CMMS Software Inc., Privacy Officer
Companion to	Annex 3 of the AssetLab Data Processing Agreement; Section 8.7 of the AssetLab Terms of Service
Review cycle	On any change to the sub-processor set, and annually
Supersedes	Version 1.8, 1 October 2026

This list is a public disclosure. It is not an agreement and does not vary the terms of any agreement between AssetLab and a Customer.

CONTENTS

1. What this list covers 3
2. Current sub-processors 4
3. Cross-border transfer safeguards 6
4. Optional features that create additional processing 7
5. Change notification 7
6. What is not a sub-processor 8
7. Artificial intelligence and machine learning 8
8. Version history 8
9. Contact 10

1. What this list covers

This document identifies every third-party service provider (a "sub-processor") that AssetLab engages to process Customer Data on its behalf in connection with the AssetLab platform.

Each sub-processor is bound by a written data processing agreement with obligations no less protective than those in the AssetLab Data Processing Agreement (DPA). AssetLab remains liable to Customers for the acts and omissions of its sub-processors.

This list is the canonical companion to Annex 3 of the AssetLab DPA and Section 8.7 of the AssetLab Terms of Service. The current version is published at https://assetlab.ca/trust.

2. Current sub-processors

Sub-processor	Purpose	Processing location	Data accessed	Safeguards
Supabase, Inc.	Database hosting (PostgreSQL), object storage, Edge Functions	Canada - AWS ca-central-1 (Montreal, QC) for the database, object storage and backups. Edge Functions execute in the AWS region nearest the caller unless the call specifies a region; from 21 September 2026 every AssetLab call specifies ca-central-1, enforced by a build check. Until 21 September 2026 calls originating in western Canada and outside Canada executed in the United States (us-west-2), processing the records those calls return; storage was unaffected throughout. Edge Functions do not connect to the database directly and reach the data tier over the same authenticated path as any other client. The Storage CDN is a global service with no in-region configuration. Supabase Realtime change streaming is not used (no row changes streamed since 21 September 2026; service disabled 1 October 2026).	All Customer Data (assets, work orders, vendors, custom fields, attachments, audit logs) plus mirror of user identity: Clerk user ID, name, business email, role.	DPA; SOC 2 Type II; hosted in Canada (ca-central-1); AES-256 at rest

Sub-processor	Purpose	Processing location	Data accessed	Safeguards
Clerk, Inc.	Authoritative identity store, authentication, SSO/SAML, passkeys	United States - hosted on Google Cloud Platform and Cloudflare (Clerk DPA Schedule 2)	Full identity record: name, business email, passkey registrations, session metadata, SSO configuration. Customer users sign in by email one-time code, Microsoft OAuth, enterprise SSO or passkey; customer accounts have no passwords.	DPA incorporated by reference (clerk.com/legal/dpa, upd. 2024-11-26); EU-U.S. Data Privacy Framework (self-certified); SCCs Modules 1/2/3; UK Approved Addendum; Swiss addendum; SOC 2 Type II; TIA on file
Cloudflare, Inc.	Application delivery (SPA via Workers and CDN), WAF, DNS, DDoS protection	Global edge (US-headquartered)	Request and connection logs (IP address, timestamp, user agent, path); transit traffic decrypted at the edge for firewall inspection and not stored; administrative logs for AssetLab personnel; integration client registrations persisted in a globally-replicated key-value store. The AssetLab MCP server runs as a Cloudflare Worker and executes at the Cloudflare location nearest the caller, which for AI-assistant callers is generally outside Canada. While a request is in flight it processes the asset records that request returns. Until 23 September 2026 the Customer's AssetLab API key was held for the duration of a connection (up to 24 hours) in plaintext in Cloudflare's globally replicated key-value store; from 23 September 2026 it is held there only in encrypted form, under a key derived from the connection's access token, which is itself never stored. No asset records or documents are stored at Cloudflare.	DPA forms part of the Main Agreement (v6.4, eff. 2026-04-03); Data Privacy Framework (EU-U.S., UK, Swiss) with lapse-notification duty; SCCs Modules 2/3; UK and Swiss addenda; ISO/IEC 27001; ISO/IEC 27701; PCI DSS Level 1; SOC 2 Type II; TIA on file

Sub-processor	Purpose	Processing location	Data accessed	Safeguards
Resend (Plus Five Five, Inc.)	Outbound transactional email delivery (work order, work request, preventive maintenance, contract and vendor notifications). Inbound email receiving for the optional email-to-work-request intake channel.	United States	Outbound: recipient email address; organisation name; record title; deep link. Work request message notifications also carry up to the first 600 characters of the message body; vendor and preventive-maintenance share emails carry the message composed by the sending user. In-application bug reports are delivered through Resend with the reporter's name and email address and any files the reporter attaches. Inbound (optional): sender address and display name, subject, and full message body. Resend keeps received messages for the life of the account, with no automatic deletion, and deletes them on request.	DPA incorporated by reference (resend.com/legal/dpa, upd. 2025-12-31); EU-U.S. Data Privacy Framework + UK Extension (certified); SCCs Modules 1/2/3; UK and Swiss addenda; SOC 2 Type II for the Resend Platform (Security criteria), Advantage Partners, period 1 February 2025 to 1 February 2026, unqualified opinion, report dated 5 May 2026; inbound receiving confirmed by Resend in writing as within the DPA; TIA on file
Amazon Web Services, Inc.	Offsite encrypted backup of the database, storage buckets and identity export	Canada - AWS ca-central-1 (Montreal, QC)	A complete copy of all Customer Data, held only as client-side encrypted archives. AssetLab encrypts every artefact before upload using a key pair whose private key AWS has never held; AWS stores ciphertext it has no means to decrypt.	DPA supplements the AWS Customer Agreement; SCCs incorporated by reference (Controller-to-Processor and Processor-to-Processor); contractual undertaking not to transfer data out of the selected Region; redirect-and-notify commitments on government demands; object lock immutability; TIA on file
Sentry (Functional Software, Inc.)	Application error monitoring and diagnostics	United States and other countries	Opaque user and tenant identifiers, role, component and action tags, exception messages and stack traces. IP address, user-agent and request-URL capture are disabled, and session replay is switched off. Not a store of Customer Data; diagnostic payloads only.	DPA executed 2026-08-06 (signed instrument); Data Privacy Framework; SCCs Modules 2/3; UK and Swiss addenda; PII scrubbing; sensitive data contractually prohibited; TIA on file

3. Cross-border transfer safeguards

Customer Data (assets, work orders, vendors, custom fields, attachments, audit logs) is hosted in AWS Canada Central (Montreal, Quebec) by default, and its offsite backups are held encrypted in the same region. The sub-processors above that process data in the United States operate under:

- Written DPAs with AssetLab incorporating obligations equivalent to PIPEDA and Quebec Law 25 safeguards;
- For transfers in scope of the GDPR or UK GDPR, the EU Standard Contractual Clauses under European Commission Implementing Decision (EU) 2021/914, Module Two (Controller-to-Processor), and the UK International Data Transfer Addendum where applicable;
- Independent third-party certifications, SOC 2 Type II at minimum.

Written Transfer Impact Assessments are maintained for every sub-processor and are available to Customers on request under confidentiality. The assessed residual risk for those carrying the most significant transfers is:

- **Clerk, Inc.** (identity) - residual risk assessed LOW.
- **Resend** (email) - residual risk assessed MEDIUM (Transfer Impact Assessment v1.5, 1 October 2026), driven by the optional inbound intake channel and by the Customer-authored message text and bug-report attachments carried in outbound email.
- **Amazon Web Services, Inc.** (encrypted backup, Canada-hosted) - residual risk assessed LOW.
- **Supabase, Inc. (database, Canada-hosted) - the assessment records the contractual position at Supabase DPA section 6.1 (storage and primary processing in the selected region, with carve-outs) against the verified configuration in ca-central-1.**

The statement AssetLab makes: operational data, including its backups, is stored in Canada, and from 21 September 2026 is processed in Canada by the database, object storage and Edge Functions. Two historical exceptions are disclosed above and both are remediated. From 8 June to 2 September 2026 the backup job's compute ran outside Canada; backup storage was in ca-central-1 throughout. Until 21 September 2026 Supabase Edge Functions executed in the region nearest the caller, so function processing for callers in western Canada and outside Canada took place in the United States; storage was unaffected. AssetLab does not represent that data of every category is processed only in Canada, because identity, email, error diagnostics and the MCP integration path are not. Customers subject to a statutory data-residency requirement should raise it before contract; the AssetLab Privacy Impact Assessment Input Package sets out the jurisdiction-by-jurisdiction position.

4. Optional features that create additional processing

Two platform features change the processing profile when a Customer enables them. Both are under the Customer's control and both can be disabled per tenant.

Feature	Effect when enabled	Default
Email intake (email-to-work-request)	Full inbound message content, authored by the Customer's own personnel, is transferred to Resend in the United States	Enabled per tenant by the Customer's Administrator under Settings → Email Intake, and can be turned off at any time
AI assistant integration (MCP)	Records the assistant reads are transferred to the AI provider the Customer connects, under the Customer's own account and agreement with that provider	Off

5. Change notification

AssetLab notifies Customers of a new or replacement sub-processor by:

- Updating this list with the new effective date; and
- Sending email notification to tenant Administrators who have subscribed to sub-processor change alerts.

AssetLab gives as much advance notice as it is able, and in any event notifies Customers within five (5) business days of becoming aware of the change. AssetLab's ability to give advance notice is bounded by the notice its own sub-processors give it.

Customers may object on reasonable data-protection grounds within thirty (30) days of notice. Where AssetLab cannot accommodate the objection, the Customer may terminate the affected subscription and receive a pro-rata refund of prepaid fees for the remainder of the term, consistent with Section 8.7 of the Terms of Service. The right to object and the right to terminate with a pro-rata refund are not shortened by the notice period expressed above.

To subscribe to change notifications, write to privacy@assetlab.ca with the subject line "Subscribe: Sub-processor Updates."

6. What is not a sub-processor

The following categories are intentionally excluded from this list:

- **Customer-initiated integrations.** Third-party tools the Customer connects to AssetLab via API, MCP or webhook, for example the Customer's own Microsoft Teams workspace, GIS service or AI assistant, are not AssetLab sub-processors. The Customer selects, authorises and controls these connections and holds the relationship with the provider.
- **AssetLab corporate vendors.** Tools used to run AssetLab the company (accounting, CRM, internal communications) do not receive Customer Data and are not sub-processors.
- **Marketing website hosting.** The public marketing site at www.assetlab.ca is hosted separately from the application and never receives Customer Data; the underlying hosting provider is therefore not a sub-processor. The marketing site's own service providers are named in Section 13.3 of the AssetLab Privacy Policy.

7. Artificial intelligence and machine learning

AssetLab's position, stated precisely:

- AssetLab does not transmit Customer Data to any AI or machine-learning provider of its own initiative, and does not use Customer Data to train any AI model. No AI provider is an AssetLab sub-processor.
- Where a Customer enables the AI assistant integration (MCP), records that the Customer's assistant requests are transmitted to the AI provider the Customer has chosen, under the Customer's own account and agreement with that provider. This is a Customer-initiated integration, it is off by default, and it requires deliberate administrator action to enable.
- AssetLab neither receives nor retains any output of that AI provider, and no AssetLab-side AI processing of Customer Data occurs.

Customers in regulated or public-sector environments should record in their own privacy assessment whether the MCP integration is enabled, and for which users. AssetLab recommends leaving it disabled where a statutory data-residency requirement applies.

8. Version history

Version	Date	Summary
1.0	2026-05-26	Initial publication.

Version	Date	Summary
1.1	2026-08-06	Change-notice commitment restated to notice within five business days of AssetLab becoming aware; the objection right and the pro-rata refund remedy are unchanged. Sentry (application error monitoring, United States) added to the disclosed list and treated as a notifiable change. Resend entry expanded to cover inbound email intake, live 2026-08-05, and outbound content minimisation. Transfer Impact Assessment reference added for Resend. AI position stated precisely, distinguishing AssetLab-initiated transfer (none) from the Customer-enabled MCP integration. Optional-features section and the residency representation added.
1.2	2026-08-08	Independent assurance recorded for Resend: SOC 2 Type II for the Resend Platform, Security trust services criteria, examined by Advantage Partners for the period 1 February 2025 to 1 February 2026, unqualified opinion, report dated 5 May 2026. Not a change of sub-processor and not a notifiable change.
1.3	2026-08-10	Supabase entry qualified. Supabase Realtime, Edge Functions and the Storage CDN are global services with no in-region configuration, and for a ca-central-1 project the Realtime cluster is mapped to us-east-1. Confirmed in writing by Supabase on 10 August 2026. Storage of Customer Data, its backups and the user-identity mirror remains in Canada. Not a change of sub-processor.
1.4	2026-09-03	Disclosure corrections following a code-level review of every integration on 3 September 2026. Resend: outbound entry corrected; notifications carry up to 600 characters of work request messages, user-composed share messages, and bug-report attachments, replacing the earlier statement that templates carried a link only. Clerk: password hashes removed from the data-accessed entry, since AssetLab uses no password sign-in. Resend residual risk in Section 3 restated as MEDIUM per Transfer Impact Assessment v1.3. Not a change of sub-processor set.
1.5	2026-09-17	Two changes. (1) Supabase Realtime change streaming retired: the application no longer subscribes to it (16 September 2026) and the service is switched off on the project (17 September 2026), so application records are stored and processed in Canada without the qualification introduced in version 1.3; Edge Functions and the Storage CDN remain global services. (2) GitHub, Inc. added as a retired sub-processor: from 8 June to 2 September 2026 the nightly backup job ran on GitHub-hosted build servers, on which a transient unencrypted copy of the backup existed during each run; the job moved to AWS ca-central-1 on 3 September 2026. The GitHub engagement was a notifiable change under Section 5 and is notified with this revision; the Realtime retirement is not a change of sub-processor set.
1.6	2026-09-24	Two disclosure corrections following an internal residency review on 21 September 2026. (1) Supabase Edge Function execution region: functions execute in the region nearest the caller unless the call specifies one, and no AssetLab call did; confirmed by test the same day. Every call site has specified ca-central-1 since 21 September 2026, enforced by a build check. (2) Cloudflare: the AssetLab MCP server processes the records a request returns at the Cloudflare location nearest the caller, and until 23 September 2026 held the Customer's API key in plaintext in Cloudflare's key-value store for up to 24 hours; it is now held only in encrypted form. The Supabase entry, the Cloudflare entry and the Section 3 residency statement are restated, and the AWS entry restates backup key custody. Notified to Customers under DPA Section 6.3.
1.7	2026-10-01	Resend entry clarified from Resend's written reply: inbound email receiving is within Resend's DPA, and received messages are kept for the life of the account and deleted on request. Transfer Impact Assessment reference updated to v1.5. Email intake corrected: Administrators enable it themselves under Settings, not on request. The retired GitHub, Inc. entry, carried since version 1.5 so the change was legible, is removed. No active sub-processor is added, replaced or removed, and no Customer Data moves to a new location.
1.8	2026-10-01	Corrects the Supabase Realtime dates: change streaming ended 21 September 2026 when the publication was emptied, and the service was disabled 1 October 2026; versions 1.5 to 1.7 recorded both as 17 September 2026. Clerk entry corrected: customer users sign in by email one-time code, Microsoft OAuth or enterprise SSO, and customer accounts have no passwords; the earlier statement that no password hashes are held for AssetLab users did not account for one internal account used for app store review.

Version	Date	Summary
1.9	2026-10-12	Clerk entry corrected: SCIM provisioning and multi-factor authentication removed from the purpose, and MFA factors replaced with passkey registrations in the data accessed; AssetLab offers neither SCIM nor a second sign-in factor. Passkey sign-in added. Supabase safeguards restate Canadian hosting. Section 6 refers to Section 13.3 of the Privacy Policy for the marketing website's service providers. No sub-processor is added, replaced or removed, and no Customer Data moves to a new location.

9. Contact

Matter	Contact
Privacy and data-subject coordination	privacy@assetlab.ca
Legal, contracting and DPA requests	legal@assetlab.ca
General support	support@assetlab.ca

AssetLab CMMS Software Inc. · North Vancouver, British Columbia, Canada
Version 1.9 · Effective 12 October 2026 · Published at https://assetlab.ca/trust