GAL Customer Data Processing Addendum

Scheduler Systems Ltd
scheduler-systems.com
Confidential

Table of Contents

GAL Customer Data Processing Addendum and Subprocessor List

Status: Approved Date: 2026-05-09 Owner: Scheduler Systems Ltd. Related tracker: Scheduler-Systems/legal#186 Approved by: karabil (Shay Panuilov, CEO)

This Data Processing Addendum ("DPA") is incorporated into the GAL Terms of Service and governs how Scheduler Systems processes personal data on behalf of GAL B2B customers.

This DPA is incorporated by reference into the GAL Terms of Service for all customers. Customers who require a separately signed DPA may request one by contacting privacy@scheduler-systems.com.

- "Agreement" means the GAL Terms, order form, master services agreement, or other written or electronic agreement governing Customer's use of GAL.
- "Customer Personal Data" means personal data that Scheduler Systems processes on behalf of Customer in connection with the Services.
- "Services" means GAL, including the web app, dashboard, CLI, API, GitHub App, background agent dispatch, support channels, and related services.
- "Customer" means the organization or person using the Services under the Agreement.
- "Controller", "processor", "subprocessor", "personal data", and "processing" have the meanings given under applicable data protection law.
- "Security Incident" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data processed by Scheduler Systems.
- "Subprocessor" means a third party engaged by Scheduler Systems to process Customer Personal Data on behalf of Customer.

This Data Processing Addendum ("DPA") applies between:

- Scheduler Systems Ltd., company number 517139382, an Israeli company ("Scheduler Systems", "we", "us"); and
- the customer or organization using GAL under the applicable order form, terms of service, or other Agreement ("Customer", "you").

Customer may act as a controller or processor depending on its own use of the Services. Scheduler Systems processes Customer Personal Data as Customer's processor or subprocessor, as applicable. Scheduler Systems may separately act as an independent controller for account administration, billing, security, legal, compliance, and business operations records.

This DPA applies when Scheduler Systems processes personal data on behalf of Customer in connection with GAL, including the GAL web app, dashboard, CLI, API, GitHub App, background agent dispatch, and related support services.

This DPA does not apply to personal data Scheduler Systems processes as an independent controller, such as its own account administration, billing, security, legal, or business operations records.

---

01 Schedule A: Processing Details

A.1 Subject Matter, Nature, and Purpose

Scheduler Systems processes Customer Personal Data to provide, secure, operate, support, improve, and troubleshoot GAL services requested by Customer.

The processing includes, as applicable:

- account authentication and organization membership management;
- storage and retrieval of GAL configuration, work items, and background agent metadata;
- GitHub App and workflow integration;
- encrypted credential storage and controlled credential injection for background agent execution;
- API calls to model providers authorized or configured by Customer;
- logs, telemetry, and abuse-prevention data needed to operate and secure GAL;
- customer support communications, including support chat where enabled.

Scheduler Systems will process Customer Personal Data only on Customer's documented instructions, including the Agreement, this DPA, product configuration, and Customer's use of the Services.

A.2 Duration

Scheduler Systems will process Customer Personal Data for the term of the Agreement and as long as needed to return, delete, retain, or isolate data in accordance with the Agreement, this DPA, legal obligations, backup retention, and security requirements.

A.3 Categories of Data Subjects

Customer Personal Data may relate to:

- Customer's employees, contractors, administrators, developers, and support users;
- Customer's end users where Customer chooses to process their data through GAL;
- repository contributors or issue participants whose data appears in GitHub metadata or workflow context provided by Customer;
- website visitors or support contacts who interact with Scheduler Systems support channels for GAL.

A.4 Categories of Personal Data

Depending on Customer's use of GAL, Customer Personal Data may include:

- names, email addresses, organization membership, and account identifiers;
- authentication metadata and provider identifiers;
- GitHub organization, repository, issue, pull request, workflow, and commit metadata;
- work item titles, descriptions, comments, labels, and operational status;
- encrypted credentials or API keys that Customer stores for background agent execution;
- logs, audit events, IP addresses, device/browser metadata, request metadata, and diagnostic data;
- support chat content, contact details, and page/device metadata provided via the support chat;
- any other content Customer intentionally submits to GAL.

Customer must not submit special-category personal data, regulated health data, payment card data, government identifiers, or other highly sensitive personal data to GAL unless the Agreement expressly permits that processing.

Scheduler Systems will:

- process Customer Personal Data only for the purposes described in this DPA and the Agreement;

- ensure personnel authorized to process Customer Personal Data are bound by confidentiality obligations;
- maintain appropriate technical and organizational measures for the risk of the processing;
- assist Customer, taking into account the nature of the processing, with data subject requests, security obligations, data protection impact assessments, and regulator consultations where required by law;
- notify Customer without undue delay after becoming aware of a Security Incident affecting Customer Personal Data, and provide reasonable updates as information becomes available;
- make available information reasonably necessary to demonstrate compliance with this DPA, subject to confidentiality, security, and access-control limitations;
- support reasonable audit or inspection requests by providing existing security documentation, completed security questionnaires, summaries of relevant controls, or independent audit reports where available. Any additional audit mechanism should be defined in the Agreement or enterprise order form and should be limited to reasonable frequency, notice, confidentiality, security, and non-disruption requirements;
- return or delete Customer Personal Data at termination according to the Agreement and applicable product retention schedules, unless law requires retention.

Customer is responsible for:

- providing lawful instructions for processing;
- having a valid legal basis for collecting and submitting Customer Personal Data to GAL;
- giving required notices and obtaining required consents from data subjects;
- configuring GAL consistently with Customer's legal obligations;
- ensuring credentials and repository access granted to GAL are authorized;
- avoiding submission of prohibited sensitive data unless separately agreed.

---

02 Schedule B: Security Measures

Scheduler Systems will maintain a security program designed to protect Customer Personal Data, including as applicable:

- encryption in transit;
- encryption at rest for managed cloud storage and encrypted credential stores;
- least-privilege access controls;

- audit logging for privileged and credential-related actions;
- environment separation for production and staging;
- secure secret management;
- vulnerability management and dependency review;
- backup, deletion, and incident response procedures appropriate to the service.

Specific security exhibits may be attached to enterprise order forms or trust documentation as the product matures.

Scheduler Systems is established in Israel. GAL production infrastructure uses Google/Firebase EU resources for production user data, including Firestore database gal-run-eu in europe-west3.

Where Customer Personal Data is transferred outside the EEA, UK, Switzerland, or another protected jurisdiction, Scheduler Systems will use a lawful transfer mechanism such as an adequacy decision, Standard Contractual Clauses, the UK International Data Transfer Addendum, or another mechanism recognized by applicable law.

Some subprocessors are hosted or may access data from the United States or other jurisdictions. These are listed in Schedule C below.

03 Schedule C: Subprocessors

Customer gives Scheduler Systems general authorization to engage subprocessors for the services listed below, subject to this DPA and the change-notice process in Section 8.

Scheduler Systems remains responsible for each subprocessor's processing of Customer Personal Data to the extent required by applicable data protection law. Scheduler Systems will enter into written agreements with subprocessors that impose data-protection obligations materially no less protective than those required by this DPA, taking into account the nature of the services provided by the subprocessor.

SUBPROCESSOR	PURPOSE	PERSONAL DATA CATEGORIES	PROCESSING LOCATION / NOTES
Google LLC / Google Cloud / Firebase	Cloud hosting, Firestore, Cloud Run, Cloud Storage, Realtime Database, Secret Manager,	Account data, product data, logs, credentials metadata, operational data	EU (europe-west3) and global infrastructure. DPA accepted via Google Cloud Console.

SUBPROCESSOR	PURPOSE	PERSONAL DATA CATEGORIES	PROCESSING LOCATION / NOTES
	logging and related infrastructure		
GitHub, Inc.	GitHub App integration, repository/workflow metadata, Actions runners, workflow logs, background agent execution contexts	GitHub account and organization identifiers, repo metadata, issue/PR/workflow metadata, logs, submitted content	US-hosted. Used when Customer connects GAL to GitHub or dispatches GitHub-backed workflows.
OpenAI, L.L.C.	AI model API processing for customer-authorized OpenAI/Codex workflows	Prompt/input content, output content, API metadata	US-hosted. Applies only where Customer configures or authorizes OpenAI processing.
Anthropic, PBC	AI model API processing for customer-authorized Claude workflows	Prompt/input content, output content, API metadata	US-hosted. Applies only where Customer configures or authorizes Anthropic processing.
Google LLC / Google AI / Vertex AI	AI model API processing for customer-authorized Gemini or Google model workflows	Prompt/input content, output content, API metadata	Applies only where Customer configures or authorizes Google AI processing.
Intercom R&D Unlimited Company and affiliates	Support chat, customer support workflow, support history, technical identifiers	Contact details, support messages, page/device metadata, technical identifiers	US-hosted (app.intercom.com). Relies on Intercom DPA and Standard Contractual Clauses for GDPR compliance. DPA: https://www.intercom.com/legal/data-processing-agreement

SUBPROCESSOR	PURPOSE	PERSONAL DATA CATEGORIES	PROCESSING LOCATION / NOTES
PostHog, Inc.	Product analytics and usage telemetry	Usage events, device/browser metadata, account or organization identifiers	US-hosted. Acts as processor. DPA available at app.posthog.com/legal. EU-US Data Privacy Framework participant.
Stripe, Inc.	Billing, invoicing, subscription management, payment processing	Billing contact details, organization details, subscription metadata, payment metadata	Global. Acts as both processor (for payment processing on your behalf) and independent controller (for fraud prevention, compliance, business operations). DPA incorporated into Stripe Services Agreement. EU-US Data Privacy Framework participant.
Brevo	Transactional email delivery, delivery-status webhooks, and email suppression events	Email addresses, message metadata, delivery status, unsubscribe and bounce events	Global infrastructure. Used for GAL transactional email and related webhook reporting.

Scheduler Systems will maintain a public or customer-accessible subprocessor list and provide at least thirty (30) days' advance notice before authorizing a new subprocessor whose engagement materially expands the scope of Customer Personal Data processing.

Notice may be given by email to Customer's account owner, in-product notice, or another written notice channel designated in the Agreement.

Customer may reasonably object during the notice period on data-protection grounds. Scheduler Systems will work in good faith to address the objection. If the parties cannot reasonably resolve the objection, Customer may terminate the affected services according to the Agreement.

Emergency replacements, security-driven replacements, and legally required changes may take effect sooner where necessary, with notice provided as soon as practicable.

Notice Template

Subject: GAL subprocessor update notice

Scheduler Systems plans to add or materially change a GAL subprocessor.

- Subprocessor:

- Service purpose:
- Data categories:
- Processing location:
- Expected effective date:
- Transfer mechanism / DPA status:
- Customer action:

If you object on data-protection grounds, contact privacy@scheduler-systems.com within thirty (30) days of this notice.

For questions about this DPA or data processing practices, contact:

Scheduler Systems Ltd. Email: privacy@scheduler-systems.com