

Data Processing Agreement

Gate Intelligence AB · v1.3 · updated 2026-10-22 · gate.software/legal/dpa

Version 1.3, 22 October 2026. This is the Data Processing Agreement GATE offers its business customers. It describes **Stable** deployments, the release track built for business customers. A Customer runs on **Edge** until it moves to Stable; where Edge differs from this agreement, **Annex 4** says how. Items not yet resolved on either track are marked **Open item**. To sign it, or to ask about it, email legal@gate.software.

This Data Processing Agreement (“DPA”) forms part of the agreement between the Customer and Gate Intelligence AB for the use of GATE (the “Agreement”). It is entered into in accordance with Article 28 of Regulation (EU) 2016/679 (the “GDPR”).

1. Parties and roles

Processor: Gate Intelligence AB, org.nr 559592-1395, Ankargränd 2, 111 29 Stockholm, Sweden (“GATE”).

Controller: the customer organization identified in the Agreement or in the signature block below (the “Customer”).

For the personal data the Customer and its users put into GATE, or connect to GATE, the Customer is the controller and GATE is the processor. For the Customer’s own account, billing and usage data, GATE is an independent controller and its Privacy Policy at gate.software/legal/privacy applies.

2. Definitions

Terms written with a capital letter and not defined here have the meaning given in the Agreement. “Personal Data”, “Processing”, “Data Subject”, “Personal Data Breach”, “Supervisory Authority” and “Sub-processor” have the meaning given in the GDPR. “Customer Data” means all Personal Data that GATE Processes on behalf of the Customer under the Agreement. “Annex” means an annex to this DPA.

3. Subject matter, duration, nature and purpose

The subject matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects are set out in **Annex 1**. GATE Processes Customer Data only for the purpose of providing GATE to the Customer as described in the Agreement and this DPA.

4. GATE’s obligations as processor

4.1 Instructions. GATE Processes Customer Data only on the Customer’s documented instructions, including with regard to transfers to a third country, unless required to do so by Union or Member State law to which GATE is subject; in that case GATE informs the Customer of that legal requirement before Processing, unless the law prohibits it on important grounds of public interest. The Agreement, this DPA, and the Customer’s and its users’ use of GATE (each message, connection, setting and request made in the product) are the Customer’s documented instructions. GATE informs the Customer without delay if, in GATE’s opinion, an instruction infringes the GDPR or other data protection law.

4.2 Confidentiality. GATE ensures that every person authorised to Process Customer Data has committed to confidentiality or is under an appropriate statutory obligation of confidentiality.

4.3 Security. GATE implements the technical and organisational measures set out in **Annex 3**, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk to Data Subjects, so that the Processing meets the requirements of Article 32 of the GDPR. GATE may update Annex 3 provided the level of protection is not reduced.

4.4 Sub-processors. The Customer gives GATE general authorisation to engage the Sub-processors listed in **Annex 2**. GATE imposes on each Sub-processor, by contract, data protection obligations that provide at least the level of protection required by this DPA. GATE remains fully liable to the Customer for the performance of each Sub-processor. GATE notifies the Customer by email to the account address on file, and by publishing the change at gate.software/legal/subprocessors, before adding or replacing a Sub-processor: on **Stable**, at least 30 days before the change takes effect; on **Edge**, on the day of the change and before it takes effect. The Customer may object on reasonable data protection grounds within 30 days of the notice. On Edge, the Customer acknowledges that it has chosen a rapidly iterating service and that same-day notice is the opportunity to object it agreed to; on an objection, GATE stops using the new Sub-processor for the Customer's organization or moves the Customer to Stable. If GATE can do neither, the Customer may terminate the Agreement for the affected service and GATE refunds any unused prepaid balance. In a security emergency or when required by law, GATE may replace a Sub-processor faster and notifies the Customer as soon as practicable.

4.5 Data subject rights. Taking into account the nature of the Processing, GATE assists the Customer with appropriate technical and organisational measures, insofar as possible, in responding to requests from Data Subjects exercising their rights under Chapter III of the GDPR. GATE forwards any such request it receives directly to the Customer without undue delay and does not respond to it except on the Customer's instruction.

4.6 Assistance. GATE assists the Customer in ensuring compliance with Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of the Processing and the information available to GATE.

4.7 Personal Data Breach. GATE notifies the Customer without undue delay, and in any case within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Data. The notification describes, as far as known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information may be provided in phases. GATE documents every Personal Data Breach and cooperates with the Customer's own notification to the Supervisory Authority and to Data Subjects.

4.8 Deletion and return. On termination or expiry of the Agreement, GATE deletes all Customer Data, or returns it to the Customer and then deletes it, at the Customer's choice made within 30 days of termination; if no choice is made, GATE deletes. Deletion is complete within 30 days of the request, and copies in backups roll off within 7 days after that (Annex 3). GATE may retain Customer Data only to the extent Union or Member State law requires, and only for as long as it requires.

4.9 Audits. GATE makes available to the Customer all information necessary to demonstrate compliance with Article 28 of the GDPR, and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer. Audits take place at most once per 12 months unless a Personal Data Breach or a Supervisory Authority requires otherwise, on at least 30 days written notice, during business hours, without disrupting GATE's operations, and under confidentiality. GATE first answers by providing documentation (this DPA, Annexes, the Trust Center, and its Sub-processor terms); an on-site inspection is used where documentation does not resolve the question. Each party bears its own costs.

4.10 Records. GATE keeps a record of the Processing activities carried out on behalf of the Customer as required by Article 30(2) of the GDPR.

5. Customer's obligations as controller

The Customer is responsible for the lawfulness of the Processing, including having a legal basis for the Customer Data it puts into or connects to GATE, for informing Data Subjects, for the accuracy and minimisation of Customer Data, and for its instructions being lawful. The Customer is responsible for the accounts, settings and permissions its users configure in GATE, including which third-party services they connect and which AI models they select.

6. International transfers

GATE Processes and stores Customer Data inside the EU/EEA, with the exceptions listed in Annex 2. Where a Sub-processor Processes Customer Data outside the EU/EEA, the transfer is made under the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914, module two or three as applicable) as incorporated in GATE's agreement with that Sub-processor, together with the supplementary measures described in Annex 2, or under an adequacy decision where one applies (including the EU-US Data Privacy Framework for certified recipients). GATE does not transfer Customer Data outside the EU/EEA on any other basis without the Customer's instruction.

Some optional Sub-processors listed in Annex 2 have no transfer mechanism with GATE and are off by default: z.ai and Moonshot offer none, and Higgsfield offers a data processing agreement and Standard Contractual Clauses only under an enterprise agreement, which GATE does not have yet. If the Customer's organization owner turns on providers in China or providers that may train on data, the Customer instructs that transfer and is responsible, as controller, for its lawful basis under Chapter V GDPR; GATE carries it out on that instruction.

7. Access by GATE staff

GATE staff, and the operational bots GATE runs to operate the platform, may access Customer Data only to the extent necessary to provide, operate, support and secure GATE, to carry out the Customer's instructions, and to comply with law. The current scope of that access on Edge, on Stable and on dedicated infrastructure is described in Annex 3, section "Access control". GATE does not use Customer Data to train machine learning models. A Sub-processor that GATE classifies as training on data it receives is used only after an organization owner explicitly turns on "Allow providers that may train on your data"; it is off by default. Annex 2 names each one, and names the two whose terms allow training by default where this opt-in does not yet apply (open items).

Release tracks. GATE runs on two release tracks. **Edge** is a rapidly iterating service: it runs the newest accepted code and may add or replace Sub-processors at short notice. **Stable** changes slowly, only with changes already proven on Edge, under tighter control. Edge is opt-in: a Customer that uses GATE on Edge chooses Edge and its terms, including the Edge notice rule in section 4.4, and a Customer runs on Edge until it moves to Stable. A Customer may ask to move to Stable at any time. On Edge, GATE staff may also review Customer Data to improve GATE. GATE decides that purpose itself, so for that review GATE is an independent controller under Article 28(10) GDPR, not the Customer's processor, and relies on legitimate interest as set out in section 11a of its Privacy Policy. On Stable, staff access is limited to the purposes in the first paragraph of this section, and GATE holds no standing access to Customer Data: GATE staff and operational bots open it only when the Customer asks, case by case, and that access ends when the work does. Nothing GATE sees on Stable is used to improve GATE.

8. Liability

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement, except where the GDPR does not permit a limitation. Each party is liable to Data Subjects as set out in Article 82 of the GDPR.

9. Term and precedence

This DPA applies for as long as GATE Processes Customer Data under the Agreement and survives termination until all Customer Data has been deleted or returned. In case of conflict, this DPA prevails over the Agreement for the subject of data protection, and the Standard Contractual Clauses prevail over this DPA.

10. Governing law and disputes

This DPA is governed by Swedish law. Disputes are settled by the courts of Sweden with Stockholm District Court (Stockholms tingsrätt) as first instance, without prejudice to the rights of Data Subjects and Supervisory Authorities under the GDPR.

11. Contact

Privacy, data protection and security matters: legal@gate.software.

Signatures

Gate Intelligence AB	Customer
Name:	Name:
Title:	Title:
Date:	Date:
Signature:	Signature:

Annex 1. Description of the Processing

Subject matter. Provision of GATE, an AI agent platform in which the Customer’s users run bots that chat, remember, and act on the Customer’s connected accounts and data.

Duration. The term of the Agreement, plus the deletion period in section 4.8.

Nature of the Processing. Collection, storage, retrieval, analysis by AI models, generation of text, images, audio and video, transmission to connected third-party services on the user’s instruction, deletion.

Purpose. Providing the GATE service to the Customer as configured and instructed by its users.

Categories of Data Subjects. The Customer’s employees and users of GATE; the Customer’s customers, prospects, leads, suppliers and other contacts whose data appears in connected mailboxes, calendars, files, CRM records, messaging channels and meetings; any person mentioned in content the Customer’s users put into GATE.

Categories of Personal Data, per surface (a surface is only in scope when the Customer uses it):

Surface	Personal Data
Chat and memory	Names, contact details and any personal data users write into chats or bots save into memory; uploaded files; bot replies and tool results
CRM	Leads, contacts, companies, activities, notes, email addresses, phone numbers, email bodies of tracked conversations
Mail (Gmail, Microsoft 365)	Email headers, bodies and attachments read or drafted on the user’s instruction; the chat keeps an excerpt of each result and the bot’s working transcript keeps what was read (2 KB in chat, full result in the transcript for 30 days)

Surface	Personal Data
Calendar	Event titles, times and attendees, synced on a rolling window for scheduling (7 days back, 60 ahead)
Files (Drive, OneDrive, uploads, resources)	Any personal data inside documents the user connects or uploads
WhatsApp	Phone numbers, message text, media of linked numbers and activated chats
Slack	Messages and files in channels the bot is a member of
Meet	Audio and video streamed during a meeting; transcripts and summaries when a bot is in the room
Voice	Text sent for speech synthesis; the audio of replies read aloud
Sites, mockups, forms	Data submitted by visitors to sites the Customer publishes through GATE

Special categories of data (Art. 9) and criminal-offence data (Art. 10). Not intended. GATE is not designed for special-category data under Article 9 GDPR (such as health or biometric data) or for personal data relating to criminal convictions and offences under Article 10, and the Customer must not put such data into GATE without a separate written agreement.

Not Customer Data. GATE's own account, billing and audit data (user names, emails, roles, IP addresses, user agents, timestamps, actions taken, billing contact and payment data) is processed by GATE as controller under its Privacy Policy, not under this DPA. Stripe Payments Europe, Limited (Ireland) processes payment data as GATE's processor for that purpose.

Annex 2. Sub-processors and transfers

Authorised Sub-processors at the date of this DPA. The live list is at gate.software/legal/subprocessors. Where a provider may train on data, or has no transfer mechanism, this Annex says so, and the organization settings below decide whether it is used.

Always in the path

Sub-processor	Entity, location	Purpose	Data	Transfer mechanism	Training on data
Anthropic Ireland, Limited	US processing	Claude models: chat, code sessions, memory synthesis, message classification	Chat content, connected-account content read during a task, files, code	SCCs where Anthropic's terms for the account used provide them	Anthropic's terms for the account used apply; under its Commercial Terms (API), no
Hetzner Online GmbH	Nuremberg and Falkenstein, Germany; Helsinki, Finland	Hosting, database, file storage, backups, meeting media server	All Customer Data	None needed (EU). Hetzner's Article 28 agreement (v1.2) is signed for the GATE Intelligence AB account that Stable deployments run on	No
Cloudflare, Inc.	US, global edge	DNS, reverse proxy and TLS termination at the edge, bot protection	Traffic in transit	SCCs plus EU-US DPF (Cloudflare DPA)	No
Postmark (AC PM LLC)	US	Transactional email: sign-in links, invites, notifications	Email address, notification text	EU-US DPF plus SCCs (Postmark DPA, incorporated in its terms)	Open item: Postmark's current terms allow internal use of message content "to train and improve the Service".

Sub-processor	Entity, location	Purpose	Data	Transfer mechanism	Training on data
					Notification emails contain message text. GATE is evaluating an EU-hosted replacement
TypeSafe AI, Inc.	US	Automated quality scoring of bot replies; memory consolidation	The user message and the bot reply being scored; memory note text	SCCs (TypeSafe DPA, incorporated in its MCA)	No model training; telemetry retained

Only when the Customer uses the feature

Sub-processor	Entity, location	Purpose	Trigger	Transfer mechanism	Training on data
Composio (Sampark, Inc.)	US	Holds OAuth tokens and relays API calls for Google, Microsoft and other integrations	When a user connects an integration	SCCs (Composio DPA). Each Stable deployment uses its own Composio account on a plan that includes Composio's DPA and zero data retention	No training clause; execution logs with request and response data kept up to a year unless "Don't store data" is switched on
Google Cloud EMEA Limited (Gemini)	US processing	Transcription of voice notes and meetings, live speech in GATE Meet, image and video generation	When those features are used (transcription and images are the default engines)	EU-US DPF plus SCCs (Google processor terms)	No on the paid tier
OpenAI Ireland Ltd	US processing	Codex models when a user selects one; meeting summaries; speech-to-text fallback; images or video if selected	When selected or when Claude is unavailable	SCCs (OpenAI DPA)	OpenAI's terms for the account used apply; under its API Business Terms, no
Eleven Labs Inc.	US	Text-to-speech, speech-to-text, voice cloning, music and sound effects	When voice or sound features are used	SCCs plus DPF (ElevenLabs DPA, incorporated)	No: the data-use opt-out is set on GATE's ElevenLabs account. On by default; an organization can switch voice providers off
GitHub, Inc.	US	Repository access for code sessions and site builds; issues and pull requests written by bots	When the Customer connects a repository	EU-US DPF plus SCCs (GitHub DPA)	No (Business terms)
Apple Inc.	US	Push notifications to the GATE iPhone app	When a user installs the app	SCCs / DPF (Apple)	No
Decodo (UAB Data troops)	Lithuania (EU)	Residential proxy for the bot browser	Only if the organization selects it	None needed (EU)	Not stated
z.ai (Jingsheng Hengxing Technology Pte. Ltd.)	Singapore per its terms; Chinese parent	Chat fallback when Claude and Codex are unavailable	Off by default. Only when an organization owner turns on "Allow providers in China"	None: its terms name no SCCs or adequacy decision	No for API (opt-in)

Sub-processor	Entity, location	Purpose	Trigger	Transfer mechanism	Training on data
Moonshot AI Pte. Ltd. (Kimi)	Singapore per its terms; Chinese parent	Chat when a user selects a Kimi model	Off by default. Only when an organization owner turns on both “Allow providers in China” and “Allow providers that may train on your data”	None: no DPA exists for self-serve	Yes by default
Higgsfield Inc.	US	Video generation	Off by default. Only when an organization owner turns on “Allow providers that may train on your data”	None on GATE’s current account. Higgsfield offers a DPA and SCCs under an enterprise agreement, which GATE does not have yet	Yes, by default (not on an enterprise agreement)

Services the Customer connects with its own account are not Sub-processors of GATE. This covers the Customer’s own Gmail, Google Drive, Microsoft 365, HubSpot, Pipedrive, Notion, Shopify, Apollo, Brevo, SendGrid, Meta, Slack, Fortnox, Replicate, Luma and OpenRouter accounts, and the Customer’s own AI model accounts (for example an Anthropic or OpenAI subscription or API key). GATE connects to them on the Customer’s instruction and passes data to and from them as instructed. The Customer’s own agreement with each service governs what that service does with the data; GATE does not act as their processor or modify those terms. A Customer that runs GATE on its own Claude subscription therefore gets the same terms, data controls and settings it has when it uses Claude directly. GATE recommends turning off “Help improve our AI models” under Settings > Privacy in that Claude account (<https://claude.ai/settings/data-privacy-controls>).

Supplementary measures for transfers outside the EU/EEA: TLS in transit; only the content needed for the current task is sent to a model; contractual no-training commitments where they exist (Annex above); the Customer’s control over which integrations and optional providers its organization uses; no customer content is sent to a Sub-processor for GATE’s own purposes.

Annex 3. Technical and organisational measures (TOMs)

As they are on 2026-09-30, verified in code. A line marked “gap” is a known shortfall the Customer is told about rather than a promise.

Encryption in transit. TLS for all traffic; Cloudflare terminates at the edge for proxied hosts and re-encrypts to the origin; Caddy with Let’s Encrypt certificates on the origin; HSTS set. Minimum TLS version is the server default (1.2+).

Encryption at rest. API keys, integration tokens, vault secrets, GitHub and Slack tokens, MCP tokens and WhatsApp session credentials are encrypted with AES-256-GCM under a managed keyring. Google and Microsoft OAuth tokens are held by Composio and never stored by GATE. Gap: the Claude and Codex sign-in files used by bots are plain files readable by the bot’s own system account and server administrators; Slack’s install payload keeps a token copy in plaintext; the server disk itself is not separately encrypted.

Access control. Platform roles (administrator, master administrator) and organization roles (owner, member). Each bot runs as its own isolated system user with scoped tokens and its own home directory. Organizations are logically segregated by organization id in one database; one organization’s bots cannot reach another’s data. On Edge, named Gate Intelligence staff and the operational bots they run can open Customer Data to operate, support and secure GATE. On Stable and on dedicated infrastructure GATE holds no standing access: GATE’s tools on a Stable server reach its health, logs and services, not Customer Data, and Customer Data is opened

only when the Customer asks, case by case. Every read of a customer chat by GATE staff or an operational bot writes an audit record, and the organization owner sees those records in the organization's access log.

Authentication. Passwordless: emailed sign-in link (10 minutes), passkeys, Google or Microsoft sign-in. A session lapses after at most 30 days without use and ends after 180 days at the latest. Bots authenticate with scoped tokens.

Logging and monitoring. Administrative and authentication events in an audit log kept 90 days; secret reads in a vault access log; every tool call a bot makes is visible in the chat; bot activity events kept 30 days; platform monitoring.

Change management. All code changes go through version control, pull request review and continuous integration before production.

Backups and availability. Backups are Hetzner's server backups: a daily image of the production server, taken by Hetzner outside the server, covering the database and files on its disk together. Hetzner keeps the last 7 daily images. A restore brings back the whole server to the moment of the image. Gap: data on the server's separate storage volume is not part of a server backup.

Data minimisation towards AI models. A bot sends a model only the context of the current task. The chat keeps the first 2 KB of each tool result; the bot's own working transcript keeps the full result on GATE's server for 30 days by default. Memory search embeddings are computed locally on GATE's server, not by a vendor.

Retention. Chat messages, memories, CRM records, Slack copies, calendar events and uploaded files are kept until deleted by the Customer or on the Customer's request. WhatsApp messages are kept 30 days by default (configurable 1 to 3650 days, or not stored). Captured model requests 7 days. Session transcripts 30 days. Voice audio of read-aloud replies is kept with the message.

Deletion. Deletion of an organization removes its rows across the database on the owner's request; deleting a chat hides it and its messages are erased on request; disconnecting an integration revokes its token at Composio. A user can delete their own account under Settings > Account; a deleted chat is erased for good after a grace period, currently 60 days. Gap: no self-service data export yet, so a copy of Customer Data is provided on request to legal@gate.software; other erasure requests are handled by GATE staff within 30 days and confirmed by email; a restore from backup does not re-apply deletions made after the backup, so erased data can reappear for up to the backup retention period unless the erasure log is re-run.

Incident response. Security events are triaged by GATE's operators; the Customer is notified within 48 hours of GATE becoming aware of a Personal Data Breach (section 4.7); where GATE is controller it notifies IMY within 72 hours. Gap: the written incident procedure is being drafted.

Personnel. Staff and contractors with production access are bound by confidentiality. Production access is limited to named individuals (list held by GATE, available to the Customer on request).

Sub-processor management. The list in Annex 2 is published at gate.software/legal/subprocessors; changes are notified by email as section 4.4 sets out (on Stable at least 30 days in advance, on Edge on the day of the change); every Sub-processor is under a written data protection agreement or terms incorporating one, except where Annex 2 says otherwise.

Annex 4. Edge deployments

Edge is GATE's rapidly iterating release track (section 7). A Customer that uses GATE on Edge chooses Edge, and on Edge the following differ from the rest of this agreement. Everything not listed here applies to Edge unchanged.

Topic	Stable (this agreement)	Edge
Sub-processor changes	Notified at least 30 days before they take effect (section 4.4)	Notified on the day of the change, before it takes effect (section 4.4)
Staff access	No standing access; Customer Data is opened only when the Customer asks, case by case, to provide, operate, support and secure GATE (section 7)	Staff and operational bots can open Customer Data, and staff may also review Customer Data to improve GATE, with GATE as independent controller for that review (section 7)
Hosting accounts	All servers and backups run under the Hetzner account covered by the signed Article 28 agreement (Annex 2)	Some servers and their backups run under other Hetzner accounts that are not yet covered by that agreement
Integration relay (Composio)	Own Composio account per deployment, with Composio's DPA and zero data retention (Annex 2)	GATE's shared Composio account; its execution logs may keep request and response data for up to a year

A Customer may ask to move from Edge to Stable at any time by emailing legal@gate.software.