Data Processing Agreement

Spektal GmbH, Stau 123, 26122 Oldenburg - Version 2026-11-09

This agreement applies between the Customer as controller and Spektal GmbH as processor. It is part of the Terms of Service and is formed with their acceptance (Art. 28(9) GDPR: electronic form). This English version is a reading aid; the German version is binding.

1. Contract text

(1) The standard contractual clauses of the European Commission between controllers and processors under Art. 28(7) GDPR apply, Commission Implementing Decision (EU) 2021/915 (https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj), Clauses 1 to 10 in the official language version. They are incorporated unchanged and prevail over everything else in this agreement and in the Terms in the event of a contradiction. Annexes I to IV below complete them.

(2) The options: Clause 5 (docking) is not used. Clause 7.7(a) Option 2 (general written authorisation) applies with the period in section 3.

2. Instructions and cooperation

(1) The processor processes only on documented instructions. Instructions are the controller's use of the platform (deploying, configuring, deleting, also through the API) and messages in text form to privacy@rytiv.com.

(2) The processor reports a personal data breach without undue delay to the registered address. It forwards requests of data subjects that reach it; the platform provides the means to view, correct and delete the controller's data.

(3) The processor provides evidence (these annexes, logs of operator actions, certificates of sub-processors where available) on request in text form. Audits on site are possible under Clause 7.6; reasonable notice is as a rule 30 days, and they may not impair other customers. The processor checks the data centres of sub-processors through their reports.

(4) If an authority of a third country demands access to data, the processor informs the controller as far as allowed, and discloses data only on a basis effective in the EU.

3. Sub-processors

(1) The controller authorises the sub-processors named in Annex IV.

(2) The processor announces a change or an addition at least 30 days in advance by email to the registered address and publishes it on this page.

(3) The controller may object for a reason of data protection law within 14 days of the notice. If the parties find no solution within a further 14 days, the controller may terminate the affected service or the contract without notice; section 8(6) of the Terms applies.

(4) The processor binds sub-processors to equivalent duties and is liable for them under Art. 28(4) GDPR. It bases transfers to third countries on the ground named in Annex IV.

Annex I: Parties

Controller: the Customer, with the details of its account. Contact: the registered address. Signature: the acceptance under section 2 of the Terms.

Processor: Spektal GmbH, Stau 123, 26122 Oldenburg, Germany. Data protection contact: privacy@rytiv.com. Signature: making this agreement available; a countersigned copy on request to legal@rytiv.com.

Annex II: Description of the processing

Subject and purpose. Providing the platform: running applications in virtual machines, operating databases and object storage, delivery through the edge, sending and receiving email, billing of usage, protection against abuse.

Nature. Storing, executing, transferring and deleting data the controller brings in or that arises from running its applications. The processor does not look at the content and does not search it. An exception exists only where a concrete report or an order of an authority requires it. To fend off abuse it evaluates operating data automatically (AUP section 8).

Duration. For the term of the main contract; afterwards Annex V applies.

Data subjects. Staff and agents of the controller with access to the platform; end users of its applications; recipients of its email, who as a rule do not know of this processing.

Types of data.

- Account and access: name, email addresses of members, team name, roles, keys and tokens only as a checksum, public SSH keys, timestamps.
- Billing: quantities of use per machine, volume and bucket; credit bookings; identifiers at the payment provider.
- Operation: access logs of the edge (IP address, time, requested URL, browser identifier); access counts per address and hour without reference to a visitor; traffic totals per machine; session logs with program name and names, without values, arguments or output.
- Git: the sign-in name of the connected GitHub account, who pushed, commit messages.
- Email: recipient, subject and the complete message for delivery; incoming messages to named addresses; delivery events; suppression lists; webhook deliveries.
- The controller's content: everything in its applications, databases, volumes, buckets, logs, secrets and builds. The processor does not know this content.
- Rytiv AI, only when a person asks there: the question, identifiers and states of the team, and after approval per question masked log lines.

Special categories under Art. 9 GDPR are not collected by the platform itself. Whether the controller processes them is up to the controller.

Retention in operation.

- Messages in delivery and incoming messages: 30 days. Delivery events: 90 days. Suppression lists: bounces 12 months, complaints 24 months; platform-wide only as a pseudonym and without limit.
- Session logs, logs of agents and of access to computers: 90 days. Access counts: 30 days. Build logs: 30 days or until the application is deleted.
- Backup of the platform database: automatic snapshot 7 days (Amsterdam), encrypted copy in Paris, hourly 7 days, daily 35 days.

Annex III: Technical and organisational measures

Confidentiality.

- Separation of tenants: every resource belongs to a team; the separation is enforced in the server

logic, and unknown routes count as protected.

- Every customer application runs in its own virtual machine with its own kernel, not as a container in a shared runtime.
- API tokens and device codes are stored only as SHA-256. Secrets of applications are stored encrypted and mixed in only on delivery to the machine.
- Every sign-in to the console requires a second factor.
- Operator actions on a team are logged with time, acting person and reason. On request the controller receives the lines concerning its team.
- The internet-facing process runs without privileges and without storage credentials.

Integrity.

- TLS at the edge and to the databases.
- Exactly one writer per data carrier, secured by a lease with a fencing token; exactly one instance per machine.

Availability and resilience.

- If a server fails, machines meant to be running are restarted on another one.
- Databases on request with a standby on another server and automatic failover.
- Two or more edge nodes behind a managed load balancer.
- Rates for writing, reading and network limited per machine, a memory ceiling per machine, no overselling of booked memory.

Recoverability. Artefacts, checkpoints and volume states are in object storage; a machine can start again from them on another server. This does not replace a backup by the controller (section 7(3) of the Terms).

Review. Automated tests in the rollout path; a rollout aborts if a new version does not become healthy. Alerts on anomalies.

A limit we name openly. Customer data on disk and the platform database are currently not additionally encrypted, apart from secrets and the copy in Paris. Whoever needs this encrypts in their own application with their own keys. Business mail to our contact addresses, including abuse reports with personal data, is not on the platform but at Google (Annex IV).

Annex IV: Sub-processors

This list names the services that can see the controller's data, with location and ground. A parent based outside the EU is stated, because a reviewer reads exactly that.

Running the platform

Scaleway SAS
Address: 8 rue de la Ville l'Evêque, 75008 Paris, France
Servers, network and data centre; the managed Postgres databases of the platform and the console; object storage (artefacts, customer objects, backups); load balancer.
Location: Netherlands (Amsterdam); backup copy of the platform database in France (Paris).
Ground: EU. According to its own list, Scaleway rents data centre space in the Netherlands from operators whose parent is based in the USA (Equinix, Digital Realty, Iron Mountain); they have no logical access.

Cloudflare, Inc.
Address: 101 Townsend St, San Francisco, CA 94107, USA
Authoritative DNS for our domains, including the names of applications and their custom domains. Cloudflare only answers where a name lives; it is not in the data path and sees no content.

Location: Worldwide (anycast).
Ground: Standard contractual clauses (Commission Implementing Decision (EU) 2021/914).

Quad9 Foundation
Address: c/o SWITCH, Werdstrasse 2, 8004 Zürich, Switzerland
Recursive name resolution for outbound requests of the machines. Quad9 sees the names looked up and our servers as the asker, not the end users.
Location: Switzerland, anycast locations.
Ground: Adequacy decision for Switzerland (2000/518/EC).

Anthropic Ireland, Limited
Address: Dublin, Ireland (parent: Anthropic, PBC, USA)
AI-assisted operating tools of our operators during incidents and maintenance. It concerns operating data an operator handles in doing so: log lines, error messages, identifiers of resources. The tool's vendor itself has no access to customer databases.
Location: USA and other countries.
Ground: Standard contractual clauses through the vendor's data processing addendum.

Rytiv AI, only when switched on and asked

Fireworks.ai, Inc.
Address: 900 Concar Drive, Floor 5, San Mateo, CA 94402, USA
Language model for Rytiv AI, the optional assistant of the console. Only when a person asks it something there, and only where the installation has it switched on.
Location: USA and other countries, no region binding.
Ground: Standard contractual clauses (Commission Implementing Decision (EU) 2021/914) in the Fireworks data processing addendum. No training on customer data, no retention beyond the request.

Payment and contact addresses

Stripe acts on its own responsibility for parts of this. The mailbox behind our contact addresses holds what somebody writes to us, including abuse reports with personal data, but no workloads. Both are named here so that nothing is missing.

Stripe Payments Europe, Limited
Address: One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland (parent: Stripe, Inc., USA)
Payment processing of credit top-ups, invoices and receipts. Stripe sees billing details, amount and payment method, no workloads and no content. For parts of this Stripe acts on its own responsibility.
Location: EU (Ireland); transfers within the group under Stripe's terms.
Ground: Contract with the Irish company.

Google Cloud EMEA Limited (Google Workspace)
Address: 70 Sir John Rogerson's Quay, Dublin 2, Ireland (parent: Google LLC, USA)
The mailbox for Rytiv's business mail. Mail to our @rytiv.com addresses, such as abuse@, legal@, privacy@ and support@, goes through Cloudflare Email Routing and arrives there. This includes support requests and abuse reports with personal data of those reporting and those reported, but not customer workloads, databases or files on the platform.
Location: Stored data in Europe (data region). Processing can also take place outside the EU, for example in the USA.
Ground: Contract with the Irish company including Google's Data Processing Addendum. Transfers by Google to subprocessors outside the EEA follow section 4 of its European terms: another recognised transfer solution or standard contractual clauses.

Independent or at the Customer's choice

These are not our sub-processors. They are listed because data reaches them.

GitHub, Inc.
Address: 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA
Only when the customer chooses it: signing in with GitHub and deploying from a GitHub repository. GitHub sees these sign-ins and reads under the customer's own contract with GitHub.
Location: USA.
Ground: The customer's own contract with GitHub; not engaged by us.

Internet Security Research Group (Let's Encrypt)
Address: 548 Market St, PMB 77519, San Francisco, CA 94104-5401, USA
TLS certificates for applications and custom domains. The domain names then appear in public certificate transparency logs, the names only, no content.
Location: USA; the names are public.
Ground: An independent certificate authority; no processing on our behalf.

Immutable VOF (Oh Dear)
Address: Hemelshoek 277, 2590 Berlaar, Belgium
Public status page status.rytiv.com: checks from outside whether our services respond, processes IP address and browser data when the page is visited, and holds the email addresses of people who subscribe to status updates. Sees no workloads and no customer content.
Location: Main data in Belgium; the checks run worldwide at the provider's service providers.
Ground: Provider based in the EU, the provider's data processing agreement (version of 19 January 2026). A subscription is voluntary.

Annex V: Deletion and return

(1) The controller retrieves its data itself through the ways named in section 9(5) of the Terms. This is the return under Art. 28(3)(g) GDPR.

(2) If the controller deletes a resource, a team or its account, this counts as an instruction to delete at once. When the contract ends, the processor deletes after the retrieval period of at least 30 calendar days.

(3) Deleted data leaves the backups of the platform database after 45 days at the latest. A regular run removes data in object storage once no machine needs it any more.

(4) Billing data and evidence remain as long as the law requires: invoices and accounting vouchers 8 years, commercial books 10 years (section 147 AO, section 257 HGB). The record of accepting the terms remains until the end of the third year after the account is deleted.