Auftragsverarbeitungsvertrag

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

Dieser Vertrag gilt zwischen dem Kunden als Verantwortlichem und der Spektal GmbH als Auftragsverarbeiter. Er ist Teil der Allgemeinen Geschäftsbedingungen und kommt mit deren Annahme zustande (Art. 28 Abs. 9 DSGVO: elektronische Form). Diese deutsche Fassung ist verbindlich.

1. Vertragstext

(1) Es gelten die Standardvertragsklauseln der Europäischen Kommission für Verantwortliche und Auftragsverarbeiter nach Art. 28 Abs. 7 DSGVO, Durchführungsbeschluss (EU) 2021/915 (https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj), Klauseln 1 bis 10 in der amtlichen deutschen Sprachfassung. Sie sind unverändert einbezogen und gehen bei Widersprüchen allem Übrigen in diesem Vertrag und in den Geschäftsbedingungen vor. Die Anlagen I bis IV unten vervollständigen sie.

(2) Die Wahlmöglichkeiten: Klausel 5 (Beitritt Dritter) wird nicht verwendet. Klausel 7.7 Buchstabe a Option 2 (allgemeine schriftliche Genehmigung) gilt mit der Frist aus Abschnitt 3.

2. Weisungen und Zusammenarbeit

(1) Der Auftragsverarbeiter verarbeitet nur auf dokumentierte Weisung. Weisung sind die Nutzung der Plattform durch den Verantwortlichen (Bereitstellen, Konfigurieren, Löschen, auch über die Programmierschnittstelle) sowie Mitteilungen in Textform an privacy@rytiv.com.

(2) Eine Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter unverzüglich an die hinterlegte Adresse. Anfragen betroffener Personen, die ihn erreichen, leitet er weiter; die Plattform stellt die Mittel bereit, Daten des Verantwortlichen einzusehen, zu berichtigen und zu löschen.

(3) Nachweise (diese Anlagen, Protokolle der Betreiber-Eingriffe, Zertifikate der Unterauftragsverarbeiter, soweit verfügbar) stellt der Auftragsverarbeiter auf Anfrage in Textform bereit. Prüfungen vor Ort sind nach Klausel 7.6 möglich; angemessen ist in der Regel eine Ankündigung von 30 Tagen, und sie dürfen andere Kunden nicht beeinträchtigen. Die Rechenzentren der Unterauftragsverarbeiter prüft der Auftragsverarbeiter über deren Berichte.

(4) Verlangt eine Behörde eines Drittlands Zugang zu Daten, unterrichtet der Auftragsverarbeiter den Verantwortlichen, soweit das erlaubt ist, und gibt Daten nur auf einer in der EU wirksamen Grundlage heraus.

3. Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt die in Anlage IV genannten Unterauftragsverarbeiter.

(2) Einen Wechsel oder eine Ergänzung teilt der Auftragsverarbeiter mindestens 30 Tage vorher per E-Mail an die hinterlegte Adresse mit und veröffentlicht ihn auf dieser Seite.

(3) Der Verantwortliche kann binnen 14 Tagen nach der Mitteilung aus datenschutzrechtlichem Grund widersprechen. Finden die Parteien binnen weiterer 14 Tage keine Lösung, kann der Verantwortliche den betroffenen Dienst oder den Vertrag ohne Frist kündigen; § 8 Abs. 6 der Geschäftsbedingungen gilt.

(4) Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter auf gleichwertige Pflichten und haftet für sie nach Art. 28 Abs. 4 DSGVO. Übermittlungen in Drittländer stützt er auf die in Anlage IV genannte Grundlage.

Anlage I: Parteien

Verantwortlicher: der Kunde, mit den Angaben seines Kontos. Kontakt: die hinterlegte Adresse. Unterschrift: die Annahme nach § 2 der Geschäftsbedingungen.

Auftragsverarbeiter: Spektal GmbH, Stau 123, 26122 Oldenburg, Deutschland. Kontakt für Datenschutz: privacy@rytiv.com. Unterschrift: die Bereitstellung dieses Vertrags; eine gegengezeichnete Fassung auf Anfrage an legal@rytiv.com.

Anlage II: Beschreibung der Verarbeitung

Gegenstand und Zweck. Bereitstellung der Plattform: Ausführen von Anwendungen in virtuellen Maschinen, Betrieb von Datenbanken und Objektspeicher, Auslieferung über die Edge, Versand und Empfang von E-Mail, Abrechnung der Nutzung, Schutz vor Missbrauch.

Art. Speichern, Ausführen, Übertragen und Löschen von Daten, die der Verantwortliche einbringt oder die durch den Betrieb seiner Anwendungen entstehen. Der Auftragsverarbeiter sieht die Inhalte nicht an und durchsucht sie nicht. Eine Ausnahme besteht nur, soweit eine konkrete Meldung oder eine behördliche Anordnung das erfordert. Zur Abwehr von Missbrauch wertet er Betriebsdaten automatisiert aus (AUP Abschnitt 8).

Dauer. Für die Laufzeit des Hauptvertrags; danach gilt Anlage V.

Betroffene Personen. Beschäftigte und Beauftragte des Verantwortlichen mit Zugang zur Plattform; Endnutzer seiner Anwendungen; Empfänger seiner E-Mails, die in der Regel nichts von dieser Verarbeitung wissen.

Datenarten.

- Konto und Zugang: Name, E-Mail-Adressen der Mitglieder, Teamname, Rollen, Schlüssel und Token nur als Prüfsumme, öffentliche SSH-Schlüssel, Zeitstempel.
- Abrechnung: Nutzungsmengen je Maschine, Volume und Bucket; Guthabenbuchungen; Kennungen beim Zahlungsdienstleister.
- Betrieb: Zugriffsprotokolle der Edge (IP-Adresse, Zeitpunkt, angefragte URL, Browserkennung); Zugriffszahlen je Adresse und Stunde ohne Besucherbezug; Verkehrssummen je Maschine; Sitzungsprotokolle mit Programmname und Namen, ohne Werte, ohne Argumente, ohne Ausgabe.
- Git: Anmeldename des verbundenen GitHub-Kontos, wer gepusht hat, Commit-Nachrichten.
- E-Mail: Empfänger, Betreff und vollständige Nachricht für die Zustellung; eingehende Nachrichten an benannte Adressen; Zustellereignisse; Sperrlisten; Webhook-Zustellungen.
- Inhalte des Verantwortlichen: alles in seinen Anwendungen, Datenbanken, Volumes, Buckets, Protokollen, Geheimnissen und Bauvorgängen. Diese Inhalte kennt der Auftragsverarbeiter nicht.
- Rytiv AI, nur wenn eine Person dort fragt: die Frage, Bezeichner und Zustände des Teams, nach Freigabe je Frage maskierte Protokollzeilen.

Besondere Kategorien nach Art. 9 DSGVO erhebt die Plattform nicht selbst. Ob der Verantwortliche sie verarbeitet, liegt bei ihm.

Aufbewahrung im Betrieb.

- Nachrichten in der Zustellung und eingehende Nachrichten: 30 Tage. Zustellereignisse: 90 Tage. Sperrlisten: Bounces 12 Monate, Beschwerden 24 Monate; plattformweit nur als Pseudonym und unbefristet.
- Sitzungsprotokolle, Protokolle von Agenten und von Zugriffen auf Computer: 90 Tage. Zugriffszahlen: 30 Tage. Bauprotokolle: 30 Tage oder bis zur Löschung der Anwendung.
- Sicherung der Plattform-Datenbank: Auto-Snapshot 7 Tage (Amsterdam), Kopie in Paris verschlüsselt, stündlich 7 Tage, täglich 35 Tage.

Anlage III: Technische und organisatorische Maßnahmen

Vertraulichkeit.

- Mandantentrennung: Jede Ressource gehört zu einem Team; die Trennung wird in der Serverlogik erzwungen, unbekannte Routen gelten als geschützt.
- Jede Kundenanwendung läuft in einer eigenen virtuellen Maschine mit eigenem Kernel, nicht als Container in einer geteilten Laufzeit.
- API-Token und Gerätecodes liegen nur als SHA-256 in der Datenbank. Geheimnisse der Anwendungen liegen verschlüsselt und werden erst beim Ausliefern an die Maschine eingemischt.
- Jede Anmeldung an der Console verlangt einen zweiten Faktor.
- Betreiber-Eingriffe in ein Team werden mit Zeitpunkt, handelnder Person und Begründung protokolliert. Auf Anfrage erhält der Verantwortliche die Zeilen zu seinem Team.
- Der internetseitige Prozess läuft ohne Rechte und ohne Speicher-Zugangsdaten.

Integrität.

- TLS an der Edge und zu den Datenbanken.
- Genau ein Schreiber je Datenträger, abgesichert durch ein Lease mit Fencing-Token; genau eine Instanz je Maschine.

Verfügbarkeit und Belastbarkeit.

- Fällt ein Server aus, werden Maschinen mit Soll-Zustand "laufend" auf einem anderen neu gestartet.
- Datenbanken auf Wunsch mit Standby auf einem anderen Server und automatischer Umschaltung.
- Zwei oder mehr Edge-Knoten hinter einem verwalteten Lastverteiler.
- Raten für Schreiben, Lesen und Netz je Maschine begrenzt, Speicherobergrenze je Maschine, kein Überverkauf gebuchten Arbeitsspeichers.

Wiederherstellbarkeit. Artefakte, Checkpoints und Volume-Stände liegen im Objektspeicher; eine Maschine kann daraus auf einem anderen Server wieder anlaufen. Das ersetzt keine Sicherung durch den Verantwortlichen (§ 7 Abs. 3 der Geschäftsbedingungen).

Überprüfung. Automatisierte Tests im Ausrollweg; ein Rollout bricht ab, wenn eine neue Fassung nicht gesund wird. Alarme bei Auffälligkeiten.

Grenze, die wir offen nennen. Auf Platte liegende Kundendaten und die Plattform-Datenbank sind derzeit nicht zusätzlich verschlüsselt, abgesehen von den Secrets und der Kopie in Paris. Wer das braucht, verschlüsselt selbst in seiner Anwendung; die Anwendung kann das über eigene Schlüssel tun. Geschäftspost an unsere Kontaktadressen, auch Missbrauchsmeldungen mit personenbezogenen Daten, liegt nicht auf der Plattform, sondern bei Google (Anlage IV).

Anlage IV: Unterauftragsverarbeiter

Diese Liste nennt die Dienste, die Daten des Verantwortlichen sehen können, mit Ort und Grundlage. Sitz der Mutter außerhalb der EU steht dabei, weil ein Prüfer genau das liest.

Betrieb der Plattform

Scaleway SAS
Anschrift: 8 rue de la Ville l'Evêque, 75008 Paris, France
Server, Netz und Rechenzentrum; verwaltete Postgres-Datenbanken der Plattform und der Console; Objektspeicher (Artefakte, Kundenobjekte, Sicherungen); Lastverteiler.

Ort: Niederlande (Amsterdam); Sicherungskopie der Plattform-Datenbank in Frankreich (Paris).
Grundlage: EU. Die Rechenzentrumsflächen in den Niederlanden mietet Scaleway laut eigener Liste bei Betreibern mit Sitz der Mutter in den USA (Equinix, Digital Realty, Iron Mountain); diese haben keinen logischen Zugriff.

Cloudflare, Inc.
Anschrift: 101 Townsend St, San Francisco, CA 94107, USA
Autoritatives DNS für unsere Domains, darin die Namen von Anwendungen und deren eigene Domains. Cloudflare beantwortet nur, wo ein Name liegt; es steht nicht im Datenweg und sieht keinen Inhalt.
Ort: Weltweit (Anycast).
Grundlage: Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914).

Quad9 Foundation
Anschrift: c/o SWITCH, Werdstrasse 2, 8004 Zürich, Switzerland
Rekursive Namensauflösung für ausgehende Anfragen der Maschinen. Quad9 sieht die nachgeschlagenen Namen und unsere Server als Fragenden, nicht die Endnutzer.
Ort: Schweiz, Anycast-Standorte.
Grundlage: Angemessenheitsbeschluss für die Schweiz (2000/518/EG).

Anthropic Ireland, Limited
Anschrift: Dublin, Ireland (parent: Anthropic, PBC, USA)
KI-gestützte Betriebswerkzeuge unserer Bediener bei Störung und Wartung. Betroffen sind Betriebsdaten, die ein Bediener dabei verarbeitet: Protokollzeilen, Fehlermeldungen, Bezeichner von Ressourcen. Kein Zugriff auf Kundendatenbanken durch den Anbieter des Werkzeugs selbst.
Ort: USA und weitere Länder.
Grundlage: Standardvertragsklauseln über das Data Processing Addendum des Anbieters.

Rytiv AI, nur wenn eingeschaltet und gefragt

Fireworks.ai, Inc.
Anschrift: 900 Concar Drive, Floor 5, San Mateo, CA 94402, USA
Sprachmodell für Rytiv AI, den optionalen Assistenten der Console. Nur wenn eine Person dort etwas fragt und nur, soweit die Installation ihn eingeschaltet hat.
Ort: USA und weitere Länder, keine Regionsbindung.
Grundlage: Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914) im Data Processing Addendum von Fireworks. Kein Training mit Kundendaten, keine Speicherung über die Anfrage hinaus.

Zahlung und Kontaktadressen

Stripe handelt für Teile in eigener Verantwortung. Das Postfach hinter unseren Kontaktadressen enthält, was uns jemand schreibt, auch Missbrauchsmeldungen mit personenbezogenen Daten, aber keine Workloads. Beide sind hier genannt, damit nichts fehlt.

Stripe Payments Europe, Limited
Anschrift: One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland (parent: Stripe, Inc., USA)
Zahlungsabwicklung der Guthaben-Aufladung, Rechnungen und Belege. Stripe sieht Rechnungsdaten, Betrag und Zahlungsweg, keine Workloads und keine Inhalte. Stripe handelt für Teile davon in eigener Verantwortung.
Ort: EU (Irland); Übermittlungen im Konzern nach den Bedingungen von Stripe.
Grundlage: Vertrag mit der irischen Gesellschaft.

Google Cloud EMEA Limited (Google Workspace)
Anschrift: 70 Sir John Rogerson's Quay, Dublin 2, Ireland (parent: Google LLC, USA)
Postfach für die Geschäftspost von Rytiv. Mail an unsere Adressen @rytiv.com, etwa abuse@, legal@,

privacy@ und support@, läuft über Cloudflare Email Routing und landet dort. Das umfasst Support-Anfragen und Missbrauchsmeldungen mit personenbezogenen Daten von Meldenden und Gemeldeten, nicht aber Workloads, Datenbanken oder Dateien von Kunden auf der Plattform.
Ort: Gespeicherte Daten in Europa (Datenregion). Die Verarbeitung kann auch außerhalb der EU stattfinden, etwa in den USA.
Grundlage: Vertrag mit der irischen Gesellschaft samt Data Processing Addendum von Google. Übermittlungen von Google an Unterauftragnehmer außerhalb des EWR richten sich nach Abschnitt 4 der dortigen europäischen Bedingungen: ein anderes anerkanntes Übermittlungsinstrument oder Standardvertragsklauseln.

Eigenständig oder auf Wahl des Kunden

Diese Stellen sind keine Unterauftragsverarbeiter von uns. Sie stehen hier, weil Daten dorthin gelangen.

GitHub, Inc.
Anschrift: 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA
Nur wenn der Kunde es wählt: Anmeldung mit GitHub und Bereitstellung aus einem GitHub-Repository. GitHub sieht diese Anmeldungen und Zugriffe unter dem eigenen Vertrag des Kunden mit GitHub.
Ort: USA.
Grundlage: Eigener Vertrag des Kunden mit GitHub; kein Auftrag von uns.

Internet Security Research Group (Let's Encrypt)
Anschrift: 548 Market St, PMB 77519, San Francisco, CA 94104-5401, USA
TLS-Zertifikate für Anwendungen und eigene Domains. Die Domainnamen stehen danach in öffentlichen Certificate-Transparency-Protokollen, nur die Namen, keine Inhalte.
Ort: USA; die Namen sind öffentlich.
Grundlage: Eigenständige Zertifizierungsstelle; keine Auftragsverarbeitung.

Immutable VOF (Oh Dear)
Anschrift: Hemelshoek 277, 2590 Berlaar, Belgium
Öffentliche Statusseite status.rytiv.com: prüft von außen, ob unsere Dienste antworten, verarbeitet beim Besuch der Seite IP-Adresse und Browserdaten und hält die Mail-Adressen derer, die Statusmeldungen abonnieren. Sieht keine Workloads und keine Kundeninhalte.
Ort: Hauptdaten in Belgien; die Prüfungen laufen weltweit bei den Dienstleistern des Anbieters.
Grundlage: Anbieter mit Sitz in der EU, Auftragsverarbeitungsvertrag des Anbieters (Fassung vom 19.01.2026). Ein Abonnement ist freiwillig.

Anlage V: Löschung und Rückgabe

(1) Der Verantwortliche ruft seine Daten über die in § 9 Abs. 5 der Geschäftsbedingungen genannten Wege selbst ab. Das ist die Rückgabe nach Art. 28 Abs. 3 Buchstabe g DSGVO.

(2) Löscht der Verantwortliche eine Ressource, ein Team oder sein Konto, gilt das als Weisung zur sofortigen Löschung. Endet der Vertrag, löscht der Auftragsverarbeiter nach Ablauf der Abruffrist von mindestens 30 Kalendertagen.

(3) Gelöschte Daten fallen spätestens nach 45 Tagen aus den Sicherungen der Plattform-Datenbank. Daten im Objektspeicher entfernt ein regelmäßiger Lauf, sobald keine Maschine sie mehr braucht.

(4) Abrechnungsdaten und Nachweise bleiben, solange das Gesetz es verlangt: Rechnungen und Buchungsbelege 8 Jahre, Handelsbücher 10 Jahre (§ 147 AO, § 257 HGB). Der Nachweis der Annahme der Bedingungen bleibt bis zum Ende des dritten Jahres nach der Löschung des Kontos.