Richtlinie zur zulässigen Nutzung

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

Diese Richtlinie ist Teil der Allgemeinen Geschäftsbedingungen. Sie gilt für den Kunden, seine Mitglieder und seine Endnutzer. Diese deutsche Fassung ist verbindlich.

1. Warum es diese Regeln gibt

Rytiv läuft auf Servern und Adressen, die sich alle Kunden teilen. Ein Missbrauch trifft deshalb nie nur eine Anwendung: Eine Beschwerde kann unseren Infrastrukturanbieter (genannt in der Liste der Unterauftragsverarbeiter) veranlassen, einen ganzen Server zu sperren, und eine schlechte Adresse trifft die Zustellung aller. Die Regeln unten enthalten auch, was uns dieser Anbieter auferlegt und was wir weitergeben müssen.

2. Rechtswidrige Inhalte

Verboten ist, Inhalte zu speichern, bereitzustellen oder zu verbreiten, die gegen geltendes Recht verstoßen oder Rechte Dritter verletzen, insbesondere:

- Darstellungen sexuellen Kindesmissbrauchs und jede sexualisierte Darstellung Minderjähriger;
- terroristische Inhalte, Aufrufe zu Straftaten, Volksverhetzung und Hass wegen Herkunft, Religion, Geschlecht, sexueller Orientierung oder Behinderung, Verherrlichung von Gewalt und von Verbrechen gegen die Menschlichkeit;
- pornografische Inhalte. Das Verbot unseres Infrastrukturanbieters gilt besonders dann, wenn Minderjährige sie wahrnehmen können; Rytiv gibt es deshalb ohne Ausnahme weiter;
- Verletzungen von Urheber-, Marken- und Persönlichkeitsrechten, einschließlich der Weiterverbreitung fremder Fernseh- und Streaming-Angebote (illegales IPTV);
- Betrug, verbotene Waren und alles, was Menschen zur Selbstgefährdung anleitet.

3. Phishing und Täuschung

Verboten sind Seiten und Nachrichten, die eine fremde Identität, Marke oder Anmeldeseite vortäuschen oder Zugangs- und Zahlungsdaten abgreifen. Das gilt auch für Vorlagen und Tests, die von außen erreichbar sind.

4. Schadsoftware und Angriffe

Verboten ist:

- Schadsoftware zu speichern, zu verbreiten oder zu steuern, einschließlich Steuerservern und Botnetzen;
- in fremde Systeme einzudringen oder es zu versuchen, Passwörter durchzuprobieren, Überlastungsangriffe zu fahren oder dabei zu helfen;
- fremde Netze und Adressbereiche ohne schriftliche Erlaubnis des Inhabers zu scannen;
- Absenderadressen zu fälschen und offene Weiterleitungsdienste (Proxies, Mail-Relays) für Dritte zu betreiben;
- Sicherheitsmaßnahmen und Grenzen der Plattform zu umgehen, die Plattform zurückzuentwickeln oder andere Kunden zu beeinträchtigen.

Sicherheitstests. Eigene Anwendungen darf der Kunde testen, solange das nur seine eigenen Maschinen trifft. Tests gegen die Plattform selbst, ihre Adressen und ihre geteilten Dienste (Edge, Console, API) und

Lasttests, die sie berühren, brauchen vorab unsere schriftliche Zustimmung an security@rytiv.com, mindestens 30 Tage vorher, mit Ziel, Zeitraum und Quelladressen. Überlastungsangriffe, Täuschung von Menschen und das Fälschen von Adressen sind auch dann nicht erlaubt.

5. E-Mail: nur Transaktionsmail

Über die Mail-Schnittstelle von Rytiv darf der Kunde nur Transaktionsmail senden: Nachrichten, die eine eigene Handlung des Empfängers oder seine bestehende Beziehung zum Kunden auslöst, etwa Belege, Anmeldecodes und Benachrichtigungen zu seinem Konto.

Verboten sind Werbung, Newsletter und Marketing-Mail, auch mit Einwilligung des Empfängers. Dafür braucht der Kunde einen anderen Dienst. Spam, gekaufte Listen und Mail-Bombing sind auf jedem Weg verboten.

Ausgehender Verkehr aus Maschinen auf die SMTP-Ports 25 und 2525 ist gesperrt; eine Ausnahme gibt es auf begründete Anfrage. Die Plattform begrenzt den Versand und setzt Empfänger nach Bounces und Beschwerden auf Sperrlisten.

Bei einem Verstoß gilt Abschnitt 9: zuerst ein Hinweis, dann stoppen wir den Versand der betroffenen Domain, bei Wiederholung sperren wir das Team und kündigen zuletzt. Wir lesen dafür keine Nachrichten ohne Anlass; wir handeln auf Beschwerden, Meldungen und auffällige Zustellzahlen hin.

6. Mining und vergleichbare Lasten

Verboten sind Krypto-Mining in jeder Form, auch im Rahmen des Startguthabens, Pools und Stratum-Verbindungen, und das Belegen von Speicher für Blockchain-Netze wie Chia. Verboten ist auch Black-Hat-SEO, etwa Linkfarmen und versteckte Inhalte. Rechenzeit, die der Kunde für eigene Zwecke bezahlt, etwa Datenverarbeitung und das Training von Modellen, ist ausdrücklich erlaubt.

7. Faire Nutzung

Builds, Zertifikate, eigene Domains, ausgehender Datenverkehr und Team-Mitglieder berechnen wir nicht einzeln. Das setzt eine Nutzung voraus, die zum Betrieb der eigenen Anwendungen gehört. Nicht dazu gehören: Builds als allgemeine Rechenleistung, das Ausliefern fremder Inhalte als Download- oder Proxy-Dienst und plötzliche sehr große Lastspitzen ohne Vorwarnung. Der Kunde kündigt geplante große Lastspitzen vorher an (support@rytiv.com), damit sie nicht als Angriff gelten. Die Plattform begrenzt die Netzrate je Maschine und kann solche Nutzung drosseln. Reicht das nicht, sprechen wir den Kunden an, bevor wir mehr tun.

8. Wie wir erkennen

Wir lesen keine Inhalte ohne Anlass. Wir erfahren von Verstößen durch Meldungen und durch automatische Auswertung von Betriebsdaten: Auslastung, Verbindungsziele, nachgeschlagene Namen und Datenmengen. Beim Muster von Krypto-Mining kann das System eine Maschine automatisch pausieren; es löscht dabei nichts. Über jede andere Maßnahme entscheidet ein Mensch.

9. Was wir tun

Wir wählen die mildeste Maßnahme, die das Problem wirklich löst, und gehen in dieser Reihenfolge vor:

- Stufe 1, Hinweis. Wir schreiben an die hinterlegte Adresse, nennen den Vorfall und setzen eine Frist, die zur Schwere passt.
- Stufe 2, Einschränkung. Reagiert niemand oder reicht die Frist nicht, stoppen wir die betroffene

Maschine, Anwendung oder Sendedomain, nehmen einen einzelnen Inhalt vom Netz oder drosseln.

- Stufe 3, Sperrung. Bei Wiederholung oder wenn Stufe 2 nicht reicht, sperren wir das Team oder das Konto. Daten bleiben erhalten.

- Stufe 4, Kündigung. Bei schwerem oder wiederholtem Verstoß kündigen wir nach § 9 der Geschäftsbedingungen.

Ohne Vorwarnung und direkt auf einer höheren Stufe handeln wir, wenn Abwarten nicht vertretbar ist: bei Darstellungen sexuellen Kindesmissbrauchs, terroristischen Inhalten, aktiven Angriffen und Phishing, bei Anordnungen von Behörden und Gerichten und wenn unser Infrastrukturanbieter eine Sperre verlangt oder androht. Wir löschen Inhalte nicht als Strafe; sie bleiben als Beweis und für den Kunden erhalten, bis Gesetz oder Vertrag etwas anderes verlangen.

Über eine Maßnahme unterrichten wir den Kunden mit Begründung: was wir eingeschränkt haben, wegen welcher Tatsachen, auf welcher Grundlage, ob dabei Automatik im Spiel war und wie er widersprechen kann. Der Widerspruch geht als Antwort an abuse@rytiv.com und wird von einem Menschen geprüft. Der Rechtsweg bleibt offen.

10. Melden und Behörden

Meldungen gehen an rytiv.com/abuse (https://rytiv.com/abuse) oder abuse@rytiv.com, Sicherheitslücken an security@rytiv.com, Behörden erreichen uns unter legal@rytiv.com. Auf gesetzliche Pflicht und auf begründete Anordnung geben wir Daten an Behörden heraus; den Kunden unterrichten wir, soweit das erlaubt ist.