Acceptable Use Policy

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

This policy is part of the Terms of Service. It applies to the Customer, its members and its end users. This English version is a reading aid; the German version is binding.

1. Why these rules exist

Rytiv runs on servers and addresses that all customers share. Abuse therefore never hits only one application: a complaint can make our infrastructure supplier (named in the list of sub-processors) suspend a whole server, and a bad address hurts everybody's delivery. The rules below also contain what this supplier imposes on us and what we have to pass on.

2. Illegal content

You may not store, offer or distribute content that violates applicable law or the rights of third parties, in particular:

- depictions of child sexual abuse and any sexualised depiction of minors;
- terrorist content, calls for criminal acts, incitement and hatred on grounds of origin, religion, gender, sexual orientation or disability, glorification of violence and of crimes against humanity;
- pornographic content. Our infrastructure supplier's ban applies especially where minors can perceive it; Rytiv therefore passes it on without exception;
- infringements of copyright, trademarks and personality rights, including the redistribution of other people's television and streaming offers (illegal IPTV);
- fraud, prohibited goods and anything that instructs people in harming themselves.

3. Phishing and deception

Pages and messages that fake another identity, brand or sign-in page, or that harvest credentials or payment data, are prohibited. This also applies to templates and tests that can be reached from outside.

4. Malware and attacks

You may not:

- store, distribute or control malware, including command servers and botnets;
- break into other people's systems or try to, try passwords in bulk, run denial-of-service attacks or help with them;
- scan other people's networks and address ranges without the owner's written permission;
- forge sender addresses or run open forwarding services (proxies, mail relays) for third parties;
- get around security measures and limits of the platform, reverse engineer the platform or impair other customers.

Security testing. You may test your own applications as long as this hits only your own machines. Tests against the platform itself, its addresses and its shared services (edge, console, API), and load tests that touch them, need our prior written consent through security@rytiv.com, at least 30 days in advance, naming the target, the period and the source addresses. Denial of service, deceiving people and forging addresses are not allowed even then.

5. Email: transactional mail only

Through Rytiv's mail interface the Customer may send transactional mail only: messages triggered by the recipient's own action or by the recipient's existing relationship with the Customer, such as receipts, sign-in codes and notifications about their account.

Advertising, newsletters and marketing mail are prohibited, even with the recipient's consent. The Customer needs another service for those. Spam, bought lists and mail bombing are prohibited on every path.

Outbound traffic from machines to the SMTP ports 25 and 2525 is blocked; an exception is available on a reasoned request. The platform limits sending and puts recipients on suppression lists after bounces and complaints.

On a violation section 9 applies: a notice first, then we stop sending for the affected domain, on repetition we suspend the team and finally terminate. We do not read messages without cause for this; we act on complaints, reports and unusual delivery figures.

6. Mining and similar loads

Cryptocurrency mining in any form is prohibited, also on start credit, as are pools and stratum connections and occupying storage for blockchain networks such as Chia. Black hat SEO, such as link farms and hidden content, is prohibited too. Compute the Customer pays for its own purposes, such as data processing and training models, is expressly allowed.

7. Fair use

We do not charge separately for builds, certificates, custom domains, outbound data transfer and team members. This presumes use that belongs to running your own applications. It does not include builds as general compute, delivering other people's content as a download or proxy service, or sudden very large load spikes without warning. Announce planned large spikes in advance (support@rytiv.com), so that they do not count as an attack. The platform limits the network rate per machine and can throttle such use. If that is not enough, we talk to the Customer before we do more.

8. How we detect

We do not read content without cause. We learn of violations through reports and through automatic evaluation of operating data: load, connection destinations, names looked up and data volumes. On the pattern of cryptocurrency mining the system can pause a machine automatically; it deletes nothing in doing so. Every other measure is decided by a person.

9. What we do

We choose the mildest measure that really solves the problem, in this order:

- Step 1, notice. We write to the registered address, name the incident and set a period that fits its severity.
- Step 2, restriction. If nobody reacts or the period is not enough, we stop the affected machine, application or sending domain, take a single piece of content offline, or throttle.
- Step 3, suspension. On repetition, or if step 2 is not enough, we suspend the team or the account. Data is kept.
- Step 4, termination. For a serious or repeated violation we terminate under section 9 of the Terms.

Without warning and straight at a higher step we act where waiting is not justifiable: for depictions of child sexual abuse, terrorist content, active attacks and phishing, for orders of authorities and courts, and where

our infrastructure supplier requires or threatens a suspension. We do not delete content as a punishment; it is kept as evidence and for the Customer until law or contract require otherwise.

We inform the Customer of a measure with reasons: what we restricted, on which facts, on which ground, whether automation played a part and how to object. An objection goes as a reply to abuse@rytiv.com and is reviewed by a person. Recourse to the courts remains open.

10. Reporting and authorities

Reports go to rytiv.com/abuse (https://rytiv.com/abuse) or abuse@rytiv.com, security vulnerabilities to security@rytiv.com, and authorities reach us at legal@rytiv.com. We disclose data to authorities where the law requires it and on a reasoned order; we inform the Customer as far as this is allowed.