Acceptable use policy

Written in plain language, like our terms. It is short, it is applied consistently, and it is not negotiable — a clean network is worth more to the people running real workloads on it than a full one is worth to us.

Novogara BV, version 1.0, 11 October 2026. Kingsfordweg 151, 1043GR Amsterdam, The Netherlands · Chamber of Commerce 67854060 · VAT NL857199857B01.

1. Scope

This policy applies to every service Novogara BV ("Novogara", "we") delivers: dedicated servers, colocation and connectivity. It forms part of our terms and conditions and applies to you as the customer and to anyone who uses the service through you.

Where this policy and article 6 of the terms describe the same subject, this policy is the more detailed statement of it.

Everything here applies equally if you resell our capacity: what your customers do on our network is, towards us, what you do.

2. Your responsibility

You are responsible for everything that happens on your server and on your connection, including the conduct of anyone to whom you give access, whether or not you were aware of it at the time. Our services are unmanaged: the operating system and everything above it is yours to run and yours to secure.

If you resell our services, you are responsible for your own customers and you are expected to operate an abuse process of your own.

3. What is not permitted

The following are not permitted on our network, in any configuration:

- **Child sexual abuse material.**
- **Malware, ransomware, botnets and command-and-control infrastructure**, including loaders, droppers and control panels.
- **DDoS attacks, and the booters and stressers used to run them**, whether operated, resold or fronted from our network.
- **Spam and unsolicited bulk mail in any form**, including sending on behalf of a third party and operating the supporting infrastructure.
- **Phishing, fraud and carding**, including the pages, the panels and the resulting data.
- **Terrorism and violent extremism.**

- **Brute force attacks in any form**, against our network or any other.
- **IP spoofing and IP header modification.** Traffic leaving our network carries the address space assigned to it.
- **Using our servers as a proxy between a content server in another network and a reverse proxy service.**
- **Copyright and trademark infringement at scale**, including piracy sites, link indexes built for it and counterfeit storefronts.
- **Marketplaces and infrastructure for illegal goods** — drugs, weapons, forged documents, stolen credentials, stolen payment data or hacked accounts.
- **Unlicensed gambling, pyramid and Ponzi schemes, and investment or cryptocurrency fraud**, including the sites and panels that feed them.
- **Evading sanctions or export controls**, and any use on behalf of a sanctioned party.
- **Anything else that is not permitted under Dutch or European law.** The list above is what we see most often; it is not a loophole map. If it is illegal here, it is not allowed here.

We do not provide bulletproof hosting and we do not represent ourselves as doing so. Requests to that effect are declined.

4. What is permitted

Everything else that is lawful. We do not inspect what you run, we have no access to the data on your server and we take no position on your business model. The list in article 3 is exhaustive as far as our own rules go; beyond it, the machine and the bandwidth are yours to use as you see fit.

5. If other people publish on your service

Run a service where third parties put content online — streaming, file sharing, a forum, anything user-generated — and the material is not only your business, it is your responsibility. You are expected to be reachable, to act on a substantiated notice quickly, and to keep your own abuse address working.

Where it is needed we give you access to a takedown tool, so rights-holder notices reach you directly and you can remove the item yourself within the time the law allows. That is a far better outcome than us having to act on your behalf: you keep control of your platform, and the notice is handled by the party who can actually see the content. Ask us about it when you order, or when the first notice arrives.

A service that collects notices and does nothing with them ends up being handled at our level, and that is where suspension starts.

6. Reporting abuse

Reports go to abuse@novogara.com and are read by engineers who can act on them, every day of the year. To allow us to act without going back and forth, please include:

- the IP address or hostname, and the port where relevant;

- the date and time of the observation, including the time zone;
- supporting evidence: log lines, message headers, a URL or a sample;
- the action you are requesting.

Reports are assessed against the evidence submitted. A report that contains nothing verifiable, or a demand that has no basis in law, will be answered as such.

7. How we handle a report

We operate a notice and takedown procedure under Dutch and European law. In the ordinary course we pass the report to you and set a reasonable period in which to resolve it. Once resolved, the matter is closed.

In serious or clear-cut cases we suspend or terminate the service immediately and without prior notice, and we may remove or block access to content. Child sexual abuse material is always such a case.

Repeated violations end the agreement. Where we terminate for a violation, the fee for the remaining term of the agreement remains due.

8. Our role under European law

We deliver unmanaged infrastructure. We do not select, inspect or modify what our customers transmit or store, and we have no access to their machines. Under the European rules on intermediary services that makes us an intermediary — a conduit for the traffic we carry, and a provider of the hardware it runs on — not the publisher of anyone's content.

That is also why we have no general obligation to monitor what our customers do, and why we do not pretend to. What we do have is an obligation to act once we are given a substantiated notice, and that is exactly what article 6 and 7 describe.

Single point of contact. For authorities, for courts and for anyone using our services, that point is abuse@novogara.com for anything about content or conduct, and support@novogara.com for everything else. We correspond in English and Dutch, by email, every day of the year. There is no form to fill in and no portal to register for.

When we restrict something — suspending a service, blocking access to content — the customer gets a statement of what we did, on what ground, and on the basis of which notice or which rule, unless the law forbids us from saying so.

9. Law enforcement

Novogara BV is established in the Netherlands and acts under Dutch and European law. Lawful requests from authorities are honoured and we assist to the extent required. Send them to abuse@novogara.com with the legal basis stated; for anything urgent, say so in the subject line.

What we can hand over is limited by what we hold: the customer's own account and billing details, what they told us, and the network data our own systems keep. Our servers are unmanaged, so we do not have the contents of a customer's machine and we cannot produce what we have never had.

We do not retain data for the benefit of future requests. There is no general retention obligation for providers in the Netherlands, and we do not keep traffic histories beyond what running the network requires. A lawful order to preserve data we do hold is honoured.

Unless we are legally barred from doing so, we tell the customer that a request was made. We do not give customer details to private parties without a legal basis, and a demand from someone's lawyer is not one.

Removal orders from a competent authority — including orders concerning terrorist content or child sexual abuse material — go to abuse@novogara.com. That address is read around the clock, every day of the year, and such an order is executed within the period the law prescribes, which for terrorist content is one hour. Put the deadline in the subject line and it will be seen.

We do not operate under United States law, so the DMCA does not apply to us. A notice drafted under it is treated as an ordinary report and assessed on what it demonstrates.

10. Changes to this policy

We may amend this policy, for example when the law changes or when a new form of abuse appears. The current version is always published on this page, with its version number and date. Material changes are communicated to customers in advance.

Related documents

Terms and conditions · Uptime commitment · Privacy statement · FAQ

Novogara BV · Kingsfordweg 151, 1043GR Amsterdam, The Netherlands · Chamber of Commerce 67854060 · VAT NL857199857B01 · support@novogara.com
This document is published at https://www.novogara.com/acceptable-use and that version prevails.