

Data processing agreement

Geomodifier · Pearls and Roses OÜ

Version of 19 October 2026

Online: <https://geomodifier.com/en/dpa>

This data processing agreement is part of the terms of service (<https://geomodifier.com/en/terms>) for Geomodifier between you, the customer ("you"), and Pearls and Roses OÜ, registry code 14761524, Karu tn 39-401, 10120 Tallinn, Estonia ("we"). It applies whenever we process personal data on your behalf. You accept it together with the terms, so there is nothing to sign.

If you need a signed copy, download the PDF, sign it and send it to hello@pearlsroses.com. We sign it and send it back. The English and Estonian versions say the same; if they ever differ, the English version prevails.

1. Roles and scope

Customer Data is the personal data about your website's visitors that the service collects for you: through the gm.js tag on your pages and through the crawler visits your server reports to us. Annex 1 describes it. For Customer Data you are the controller and we are your processor.

If you use Geomodifier for someone else, such as a client whose website you run, you are their processor and we are your sub-processor. You confirm that they have allowed you to use us, and you pass this agreement on to them when they need it.

For the data of your own account, such as your email address and billing details, and for the AI answer check, we are the controller, as our privacy policy (<https://geomodifier.com/en/privacy>) describes.

This agreement applies under the EU General Data Protection Regulation (GDPR) and under any other data protection law that applies to the processing, wherever your business is, such as the UK GDPR, the Swiss Federal Act on Data Protection or US state privacy laws. Words defined in the GDPR have the meaning it gives them. Where another law names the same roles differently, for example "business" and "service provider", they mean controller and processor here.

2. Your instructions

We process Customer Data only on your documented instructions: this agreement, the terms, and the settings you choose in the workspace, such as your projects' websites and markets. This includes transfers to other countries (clause 6). If a law that applies to us requires other processing, we tell you before we start, unless that law forbids it.

If we believe an instruction breaks data protection law, we tell you at once and may hold off on it until you confirm or change it.

You are responsible for the lawfulness of the processing: you need a legal basis for it, your privacy notice tells your visitors about it, and you ask for their consent where the law that applies to you requires it, for example before gm.js runs. gm.js sets no cookies and stores nothing in the visitor's browser. Do not put anything that identifies a visitor, or any special category of personal data, into page addresses, page titles or campaign tags.

3. Confidentiality

Only people who need Customer Data to run the service can access it, and each of them is bound to confidentiality, also after their work for us ends. We use Customer Data only to provide the service to you. We do not sell it, use it for advertising, or use it to train AI models.

4. Security

We protect Customer Data with the technical and organisational measures in Annex 2. They take into account the state of the art, the costs, the nature, scope, context and purposes of the processing, and its risks to people. We may change them as technology moves on, but never so that the overall protection falls.

5. Sub-processors

You allow us to use the sub-processors in Annex 3. Before we add or replace a sub-processor of Customer Data, we tell you at least 30 days in advance by email to your account's address and on this page. You can object within those 30 days on reasonable data protection grounds. If we cannot resolve your objection, you can end the affected service before the change takes effect, and we refund what you paid for the time after it.

We bind each sub-processor by a written contract to data protection obligations that protect Customer Data at least as well as this agreement, as far as they apply to its service. We remain responsible to you for our sub-processors.

6. Transfers to other countries

We store Customer Data in the European Union: on our servers at Hetzner in Helsinki, Finland, with backups in Cloudflare's R2 storage in the EU. Cloudflare's network, which carries your visitors' requests to our servers, handles each request in the data center nearest to the visitor, which can be outside the EU.

Customer Data leaves the European Economic Area (EEA) only with a safeguard that chapter V of the GDPR accepts, such as an adequacy decision, the EU–US Data Privacy Framework or the standard contractual clauses of the European Commission (Implementing Decision (EU) 2021/914). Annex 3 names each sub-processor's safeguard.

If you are established outside the EEA in a country without an adequacy decision, module four (processor to controller) of those standard contractual clauses applies to the Customer Data we send you, such as what your workspace shows and exports. Annex 1 gives the details they need; Estonian law governs them and the courts of Estonia settle disputes about them. Where they conflict with this agreement, they prevail.

7. Helping you

We store no names, email addresses, IP addresses or cookie identifiers of your visitors, so stored data can rarely be linked to a person. If one of your visitors asks us to exercise their rights, we pass the request on to you and do not answer it ourselves unless the law requires us to. Under Setup, Your data, you can download all data of a project and delete a project with all of its data. For anything else, such as finding or deleting particular records, write to us and we do it within 14 days.

As far as the information we have allows, we help you meet your duties on security, breach notification, data protection impact assessments and prior consultation with a supervisory authority (GDPR articles 32 to 36).

8. Personal data breaches

If we become aware of a personal data breach that affects Customer Data, we tell you without undue delay and at the latest 48 hours after we became aware of it, by email to your account's address. We tell you what we know: what happened, which categories of data and roughly how many people and records it affects, the likely consequences, what we have done and propose to do, and whom you can contact. What we do not know yet, we send as soon as we learn it.

We also take reasonable steps to contain the breach and limit its harm. Telling you about a breach is not an admission of fault.

9. Information and audits

On request, we give you the information needed to show that we meet this agreement, including answers to a reasonable security questionnaire once a year.

If that is not enough, or a supervisory authority requires it, you or an independent auditor you appoint can audit us. The auditor must be bound to confidentiality and must not be our competitor. You give us 30 days' notice; the audit takes place during business hours without disrupting the service, and at most once in 12 months unless a breach or a supervisory authority makes another one necessary. Each party bears its own costs.

10. Deletion and return

We delete page views, crawler visits and alerts automatically 13 months after they are recorded. AI answer checks stay while the project exists.

Under Setup, Your data, you can download all data of a project at any time, and delete a project with all of its data. Deleting takes effect at once; copies in our backups expire within 30 days.

When this agreement ends, for example because your account is closed, we delete the remaining Customer Data within 30 days, unless you ask us for a copy first or a law requires us to keep it. Until it is deleted, this agreement still protects it.

11. Liability and precedence

Each party is liable for its own breaches of this agreement and of data protection law. The limitation of liability in the terms applies to this agreement as far as the law allows; it does not limit either party's liability towards data subjects.

If this agreement and the terms conflict about Customer Data, this agreement prevails.

12. Duration, changes and law

This agreement applies as long as we process Customer Data for you. We may update it when the law or our service changes. We tell you about a change that affects your rights by email 30 days before it takes effect; the date at the top shows the current version.

Estonian law governs this agreement, and Harju County Court in Tallinn settles disputes, as in the terms.

Signatures

For the processor: Pearls and Roses OÜ, registry code 14761524

Name and position: _____

Date: _____

Signature: _____

For the controller (customer)

Company: _____

Registry code: _____

Address: _____

Name and position: _____

Date: _____

Signature: _____

Annex 1: Details of the processing

Controller

You, the customer, as identified in your Geomodifier account. Contact: your account's email address.

Processor

Pearls and Roses OÜ, registry code 14761524, Karu tn 39-401, 10120 Tallinn, Estonia. Contact: hello@pearlsroses.com.

Subject matter and purpose

Showing you, for each of your markets, which AI crawlers fetch your pages, which AI assistants send you visitors and which visitors land on a page in another language than their browser's.

Nature of the processing

Collection (through gm.js on your pages and crawler reports from your server), storage, counting and display in your workspace, export and deletion.

Data subjects

Visitors to your website whose browser runs gm.js; people on whose behalf an AI assistant fetches your pages.

Personal data

For each page view: the page address without its query string (only the campaign tags utm_source, utm_medium and utm_campaign are kept), the page title, the referring site (only its address, or the page path when the visitor came from another page of your site), the passage an AI answer quoted when the link carries one, the page and browser language, the time, the country that Cloudflare derives from the IP address, and whether the visit looked automated (a bot or an AI agent) with a short label of what it was. For each crawler visit: the crawler's name, the page address, the response status, whether and how the crawler's address was verified, and the time.

Not stored

IP addresses (used briefly to limit requests, verify crawlers and recognise cloud networks), the user agent, cookies, device identifiers, and visitors' names and email addresses. Our web server's logs hold the time, the requested path, the status and the user agent of each request, with the address of the Cloudflare server that forwarded it instead of the visitor's, and are deleted after 14 days.

Special categories of data

None intended. Page addresses and titles can reveal an interest in a topic; we do not link them to a person.

Frequency

Continuous, while gm.js is on your pages or your server reports crawler visits.

Retention

13 months, then deleted automatically; at once when you delete the project; backups expire within 30 days.

Location

European Union: servers in Helsinki, Finland; backups in the EU. Requests pass through Cloudflare's global network.

Annex 2: Technical and organisational measures

- Encryption in transit: all traffic to geomodifier.com uses TLS (HTTPS with HSTS), and Cloudflare reaches our server over TLS with a validated certificate.
- Network: our server accepts web traffic only from Cloudflare's addresses. The database, the cache and the vector store run in a private container network that the internet cannot reach.
- Administration: remote access (SSH) is open to one allow-listed address only, and the administrator signs in with a key. The operating system installs security updates automatically.
- Sign-in: single-use email links that expire after 30 minutes; sessions in Secure, HttpOnly, SameSite=Strict cookies; links and sessions are stored only as SHA-256 hashes.
- Access control: a project's data is shown only to its owner and to our administrators. Reports from your server are authenticated with a key or an HMAC signature; requests from browsers are rate limited and must come from your site's pages.
- Data minimisation: no visitor IP addresses, cookies or device identifiers are stored; query strings are removed before storage; referrers are cut down to the referring site.
- Retention: a nightly job deletes page views, crawler visits and alerts after 13 months.
- Backups: the database is backed up every night; backups are kept for 14 days on the server, readable only by its administrator, and for 30 days in Cloudflare's R2 storage in the EU, encrypted at rest.
- Availability: health checks run every minute and alert us by email; a deployment that fails its checks is rolled back automatically.
- Change management: every change goes through version control and automated tests before it is deployed; the tests include the separation between customers' data.
- People: everyone with access is bound to confidentiality and has only the access their work needs. We handle breaches as clause 8 describes.

Annex 3: Sub-processors

These sub-processors process Customer Data. We announce changes as clause 5 describes. Stripe (payments) and OpenRouter (AI models for the monthly answer check) process data for which we are the controller, as our privacy policy (<https://geomodifier.com/en/privacy>) describes; they receive no Customer Data.

Hetzner Online GmbH

Industriestr. 25, 91710 Gunzenhausen, Germany. Hosting: the servers that run the service and store all Customer Data, in Helsinki, Finland (EU).

Cloudflare, Inc.

101 Townsend St, San Francisco, CA 94107, USA. Network and security: carries every request to geomodifier.com, including your visitors' requests from gm.js, and stores the encrypted database backups in R2 in the EU. Requests are handled in Cloudflare's data center nearest to the visitor, worldwide. Safeguards: the EU–US Data Privacy Framework and the standard contractual clauses in Cloudflare's data processing addendum.