

Attensira Data Processing Agreement

Last updated: October 27, 2026. <https://attensira.com/dpa>

Attensira Technology OÜ, Tallinn, Harju County, Estonia. Legal: legal@attensira.com. Privacy: privacy@attensira.com. Security: security@attensira.com.

This Data Processing Agreement (the DPA) is part of the Terms of Service between you (the Customer) and Attensira Technology OÜ, registered in Estonia (Attensira, we, us). It applies whenever Attensira processes personal data on your behalf while providing the Services.

It takes effect when you accept the Terms of Service, and it ends when they end, except for the duties that last longer. There is nothing to request and nothing to sign: this page is the agreement, and the PDF is the same text, to keep for your records.

1. Definitions

Words defined in the GDPR (Regulation (EU) 2016/679) have the same meaning here: controller, processor, personal data, processing, data subject and personal data breach. Words defined in the Terms of Service, such as Services and Customer Data, also keep their meaning.

- Customer Personal Data: personal data in Customer Data, or that Attensira processes for you while providing the Services.
- Subprocessor: a provider Attensira engages that processes Customer Personal Data. The current list is Annex 2.
- Data Protection Law: the GDPR, the UK GDPR and the national laws that implement or add to them, as they apply to the processing.

2. Roles

For Customer Personal Data you are the controller, and Attensira is your processor. If you use the Services for a client of yours, you may be that client's processor, and Attensira is then your subprocessor; this DPA applies the same way.

Attensira is the controller of the data it needs to run your account and bill you, and of the data of visitors to attensira.com. The Privacy Policy covers that data, not this DPA.

3. What is processed, and why

- Subject matter and purpose: providing the Services you choose: reading how your brand appears in AI answers and search, drafting work, and carrying out the work you approve or allow, including the agent actions in section 7 of the Terms of Service.
- Duration: for as long as the Terms of Service run, then until deletion under section 9.
- Nature of the processing: collecting, storing, reading, organising, analysing, drafting, sending at your direction, and deleting.
- Data subjects: your users; people who work for the sites, publications and channels you ask the agents to contact; people who reply to email sent from your mailbox; and people whose details appear on your own website or in content you give us.
- Personal data: names, business email addresses and job titles; where a contact's address was published and why they were written to; the outreach emails sent from your mailbox and the replies to them; the sender and subject of those replies, and their text only when a person in your workspace turns on reading reply text, in which case it is read to sort the reply and is not stored; user ids and the consent records your users create; screenshots of pages a browser run opened; and anything you attach or type into the Services.

- Special categories: none are needed. Do not submit special category data (GDPR art. 9) or data about criminal convictions.

4. What Attensira does

Attensira will:

- process Customer Personal Data only on your documented instructions. The Terms of Service, this DPA, and what you configure, approve or consent to in the Services are your instructions. We tell you if we believe an instruction breaks Data Protection Law, unless the law forbids telling you;
- process it for no purpose of our own, never sell it, and never use it to train AI models;
- make sure everyone at Attensira who can access it is bound by confidentiality;
- keep the security measures in Annex 1 (GDPR art. 32);
- engage subprocessors only under section 6;
- help you answer requests from data subjects (section 7) and meet your duties under GDPR arts. 32 to 36, taking into account what we know about the processing;
- delete or return the data when the Services end (section 9); and
- give you the information you need to show that these duties are met, and allow audits under section 10.

5. What you do

- You have a lawful basis for the processing you instruct, and you give the notices Data Protection Law asks of a controller.
- When you have the agents contact people, you are the sender. Outreach goes from your own mailbox under your name, and the Services enforce the outreach rules in section 7 of the Terms of Service on every message. You remain responsible for the email you approve, and for not sending it outside those rules.
- Consent for the weekly walk of your website is given by a person in your workspace who has authority over that domain.
- Your instructions comply with Data Protection Law and with the Acceptable Use Policy.

6. Subprocessors

You give Attensira a general authorisation to engage subprocessors. The current list is Annex 2. The same list, from the same source, is in section 6 of the Privacy Policy and on the security page.

- Each subprocessor is bound by a written contract with data protection duties no weaker than this DPA, and may use the data only for its part of the Services.
- Attensira stays responsible to you for how its subprocessors process Customer Personal Data.
- We notify you before adding or replacing a subprocessor, by email to your account owner and by updating Annex 2 at attensira.com/dpa, and we give the date the list last changed.
- You can object on reasonable data protection grounds by writing to legal@attensira.com before the change takes effect. We will try to resolve it; if we cannot, you can end your subscription under the Terms of Service.

7. Requests from data subjects

If a data subject asks us directly about Customer Personal Data, we pass the request to you and do not answer it ourselves unless you tell us to. You can export and delete data in the Services. Where you cannot, we help you within a reasonable time.

One exception is built in: when a person opts out of email sent through the Services, their address goes on the suppression list so no Attensira workspace writes to them again. The list keeps only a one-way hash of

each address, never the address itself, and it is kept for good so the opt-out keeps working.

8. Personal data breaches

We notify you without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. The notice describes what happened, the data and people likely affected, the likely consequences, and what we have done or propose to do, as far as we know at the time (GDPR art. 33(3)). We send what we have as soon as we have it, and follow up as we learn more.

A notice from us is not an admission of fault. Report a suspected breach or vulnerability to security@attensira.com.

9. Return and deletion

When the Services end, you have 30 days to export your data. Then we delete Customer Personal Data, unless the law requires us to keep it. Within the Services, some data is deleted sooner on a fixed schedule, published on the data retention page of the documentation. The hashed suppression list in section 7 is kept.

10. Information and audits

Write to legal@attensira.com and we give you the information reasonably needed to show compliance with this DPA, including answers to a reasonable security questionnaire.

If that information is not enough, or a supervisory authority asks, you or an independent auditor bound by confidentiality may audit the processing, with 30 days' notice, during business hours, at your cost, and no more than once a year unless a personal data breach gives cause.

11. International transfers

Attensira is in Estonia, in the EU. Some subprocessors operate in the United States. When Customer Personal Data leaves the EEA, it is protected by an EU adequacy decision, the EU-US Data Privacy Framework, or the European Commission's Standard Contractual Clauses, as set out in section 7 of the Privacy Policy.

12. General

- If this DPA and the Terms of Service conflict about personal data, this DPA wins.
- The limits of liability in the Terms of Service apply to this DPA.
- This DPA is governed by the law of Estonia, as the Terms of Service are.
- We may update this DPA, and we notify you of material changes as the Terms of Service describe. The date at the top shows the last change.

Annex 1. Security measures

- Personal data is encrypted in transit (TLS) and at rest.
- Access inside Attensira is role-based: only people who need the data to run the Services can reach it.
- API keys are shown once and stored as a hash, a revoked key fails on the next request, and sign-in to the API and MCP uses OAuth with PKCE and short-lived tokens.
- Accounts you connect, such as a mailbox, are connected by signing in on the other service's side. Attensira never asks for a password, and a password typed into a chat is removed before the message is stored.
- Agents act only within the approval mode and autonomy you set. An email, a price or a payment always waits for a person's yes.
- The weekly walk of your website runs only on your own domain, only while a person's recorded consent is

live, and only browses: it does not sign in, buy, or submit a form that sends or changes something. It never solves or bypasses a CAPTCHA.

- Data is deleted on the published retention schedule, and the suppression list keeps hashes, not addresses.

Annex 2. Subprocessors

The providers that process Customer Personal Data to run the Services. List last changed: October 27, 2026.

- Clerk: Sign-in and account authentication.
- Stripe: Payment processing.
- Autumn: Billing: plans, credit balances and usage metering.
- OpenAI and OpenRouter: The AI models that answer your tracked prompts and draft the work.
- DataForSEO: Search results and keyword data.
- context.dev and Olostep: Reading public web pages.
- Browserbase: The hosted browser for the weekly walk of your own site, run only with a person's recorded consent.
- Composio: The connector that holds the sign-ins for accounts you connect, including the Gmail or Outlook mailbox outreach is sent from.
- Hunter: Contact lookup: finds the business email of a person at a site's domain for outreach.
- MongoDB Atlas: Database.
- Railway: Application hosting and file storage.
- Vercel: Hosting for this website and the app.
- Resend: Transactional email.
- Sentry: Error monitoring.
- PostHog: Product and website analytics, and the support chat.