Privacy policy

Last updated 24 September 2026

Deltawall helps organisations keep sensitive data out of AI tools. The browser extension checks, on the employee's own device, what they paste or upload into an AI tool, and masks, blocks or warns according to the organisation's policy. This policy explains which personal data is processed along the way, by whom, why and for how long.

The key point: the text you type into an AI tool, the values that get masked, and the contents and names of files never leave your device towards Deltawall. Detection happens locally in your browser.

1. Who we are

Deltawall is provided by Deltawall B.V., registered with the Dutch Chamber of Commerce under number 42169421, with its registered address at De Boelelaan 1095 A, 1081 HV Amsterdam, the Netherlands ("we", "us").

Privacy questions or a request about your data: privacy@deltawall.ai. To report a security issue: security@deltawall.ai.

2. Our role: processor or controller

Deltawall is bought by organisations (our customers) and used by their employees. Who is responsible for the data depends on whose data it is:

- **Employee data** (their email address, department, connected browsers and the events the extension reports) is processed by us **on behalf of the employer**. The employer is the controller and sets the policy; we are the processor and act under a data processing agreement with that employer. As an employee, please exercise your rights with your employer. If you send your request to us, we forward it and help your employer handle it.
- **Administrator data** (people who use their organisation's console), data of people who sign up, and the technical data needed to run the service securely are processed by us **as controller**.

3. The browser extension

The extension only works on the AI services it has permission for: chatgpt.com, chat.openai.com, claude.ai, gemini.google.com, copilot.microsoft.com, perplexity.ai and chat.deepseek.com. The detection model ships inside the extension and runs on your device; no code or model is loaded from elsewhere.

What never leaves your device: the text you type or paste, the values that are detected and masked, and the contents and names of files you upload. A cleaned copy of a file is kept only in the browser's memory and removed after 15 minutes at most. What you finally send to the AI service goes straight from you to that service, not through Deltawall.

What the extension sends to Deltawall when it detects something (an ‘event’):

- which AI service it was (for example ‘chatgpt’), whether it was a prompt or a file, and the time;
- the kinds of data detected (for example ‘IBAN’ or ‘person's name’), how confident the detection was, the rule that applied and what happened (masked, blocked, warned, allowed);
- salted hashes of the detected values: a one-way calculation with a secret key per organisation. The value itself is not sent. Because we know the key and short values (such as a citizen service number) could in theory be recovered by trying every possibility, we treat these hashes as pseudonymised personal data, not anonymous data;
- **the reason you type yourself** when you send anyway after a warning (up to 500 characters). This text is stored with the event and visible to your organisation's administrators, so do not put sensitive data in it.

To connect the extension to your organisation, it sends your work email address (to send you a one-time code or link), a simple description of the browser (such as ‘Chrome on macOS’) and a public key. The matching private key stays in the browser. The extension also regularly fetches your organisation's policy, and tells us when it cannot find the input field on a supported AI site (only the site name and the service), so we can update the extension.

What the extension keeps on your device (in the browser's storage): the connection to your organisation, the policy and the organisation's key for the hashes, events not yet sent (at most 2,000), the last 100 messages sent so you can see on the options page what was sent, today's counters (these are not sent), your language choice and your key pair. This data is removed when you remove the extension.

If your organisation manages the browser centrally (for example through MDM), it can give the extension an enrolment token and a department.

4. The console and accounts

For the console and accounts we process:

Administrators	name, work email address, password (only as a hash), role, verification and creation dates
Organisation	name and legal name, domain(s), country, industry, size, the data protection officer's email address, chosen settings
Employees	email address, name (if the employer enters it), department and groups, status, connected browsers with their description and when they were last in contact
Events	see section 3, linked to a pseudonym of the employee rather than their name
Administrator log	which administrator did what (for example invited someone or had a pseudonym re-identified), with the email addresses or pseudonyms involved
Email	email address, subject and content of emails we send (such as sign-in links and codes), until they are sent

Events are linked to a pseudonym by default. Only the organisation can, using the features we provide for it, trace a pseudonym back to a person; that action is recorded in the administrator log. In 'browser-held identity' mode we no longer keep the link between pseudonym and email address once the employee's browsers hold a key of their own (at the latest 30 days after the mode is switched on).

5. Why, and on what legal basis

Providing the service to our customer (detection, applying policy, reporting)	For employee data: on the employer's instructions, under the data processing agreement. The employer determines its own legal basis (usually legitimate interest or a legal duty to protect data).
Creating and managing administrator accounts, signing in	Performance of the contract with the customer, and our legitimate interest in knowing who acts on behalf of an organisation
Security, preventing abuse (such as limiting sign-in attempts), fixing faults	Legitimate interest: a secure, working service
Keeping the extension working on AI sites	Legitimate interest; only the site name and service, no content
Legal obligations, such as keeping invoices for tax purposes	Legal obligation

We do not use data for advertising, do not sell it, do not build profiles from it for other purposes, and do not use customers' prompts or data to train AI models.

The extension applies the organisation's policy automatically (masking, blocking, warning). This is not a decision with legal effects or that similarly significantly affects you within the meaning of article 22 GDPR: you can change your text and send it again, and what happens with events afterwards is decided by people in your organisation.

6. Who we share data with

We only use the following sub-processors:

Google Cloud (Google Cloud EMEA Ltd., Ireland)	Hosting, database, backups, key management. The data is stored in the europe-west4 region (the Netherlands). Technical logs from servers and the load balancer, which can contain IP addresses and sometimes email addresses, are processed by Google in a logging service that is not bound to the EU; the European Commission's standard contractual clauses apply.
Resend, Inc. (United States)	Sending email, such as sign-in links, codes and invitations. Resend receives the email address and the content of the email. Transfers outside the EEA rely on the European Commission's standard contractual clauses.

Within the customer's organisation, administrators see the data the console shows, according to the roles the customer assigns. We only pass data on to others when the law requires us to.

Our staff do not look at customer data unless the customer asks us to, it is needed to investigate a security incident or abuse, or the law requires it.

7. If your organisation uses the AI gateway

Deltawall optionally offers organisations an AI gateway: a relay for their own applications that call AI models through an API. Only in that case does the content of requests pass through our servers to the AI provider the organisation has chosen (such as Mistral, Microsoft Azure, OpenAI, Anthropic or DeepSeek). That provider processes the content under its own terms and is chosen by the organisation. The browser extension does not use the gateway.

8. How long we keep data

Events, administrator log and evidence reports	90 days, unless the organisation asks for earlier deletion. After the contract ends we delete them within 90 days.
Administrator and employee accounts	For as long as the organisation is a customer and the account has not been deleted; then within 90 days
Sign-in codes, sign-in links and pairing codes	Until used or expired (minutes to hours); deleted within 24 hours after that
Content of sent emails	Wiped as soon as it is sent; the delivery record itself after 14 days
Abuse counters (by IP address or email address)	Minutes, until the time window ends
Technical logs	Up to 30 days
Database backups	Up to 14 days
A sign-up that was never confirmed	Until someone signs up again with the same domain, but no longer than 90 days; earlier on request

Invoices and other data with a statutory retention period are kept as long as the law requires (7 years in the Netherlands).

9. Security

Connections are encrypted (TLS). Passwords are stored only as a hash, and so are sign-in links and codes. The database, backups and keys are in a European cloud region. Events are recorded in a hash chain so that later changes stand out. Access within our team is limited to those who need it.

10. Cookies

We only use functional first-party cookies, none for analytics, advertising or tracking. That is why we do not ask for cookie consent.

authjs.session-token, authjs.csrf-token, authjs.callback-url	Staying signed in to the console and securing sign-in; session up to 12 hours
dw_employee	Staying signed in to your employee page; 12 hours
dw_link, dw_connect, dw_pair_code	Completing a sign-in link, connecting the extension or a pairing code; 5 to 15 minutes
dw_new_gateway_key	Showing a new gateway key once; 2 minutes

dw-lang	Remembering your language; 1 year

11. Your rights

You have the right to access, correct and delete your data, to restrict its processing, to data portability, and to object to processing based on legitimate interest.

If you are an employee of a customer, please send your request to your employer (see section 2). Otherwise, send it to privacy@deltawall.ai. We respond within one month and may ask you to confirm your identity.

If you disagree with how we handle your data, you can complain to the Dutch Data Protection Authority (https://autoriteitpersoonsgegevens.nl) or to the supervisory authority in the country where you live or work.

12. Chrome Web Store

The use of information received from Google APIs will adhere to the Chrome Web Store User Data Policy, including the Limited Use requirements. In practice: we use data only for the extension's single purpose (detecting and protecting sensitive data before it reaches an AI tool), do not transfer it except as described in this policy, do not let people read it except in the cases in section 6, and never sell it or use it for advertising, creditworthiness or resale to data brokers.

13. Changes

We update this policy when the service changes. The date of the last change is shown at the top. We tell our customers' administrators about significant changes in advance.

14. This website

This section covers the public website deltawall.ai, not the service. For the website we are the controller.

- **No cookies from this website, no trackers, no analytics.** The website itself sets no cookies; the cookies in section 10 belong to the console at app.deltawall.ai. Fonts are served from deltawall.ai itself, not from a third-party service. When the Cal.com scheduler loads in step 2 of booking a demo, or if you open it in a new tab, Cal.com and its security provider Cloudflare may set their own cookies, such as the bot-protection cookie __cf_bm.
- **What you submit.** When you request early access, a demo or a white paper, we receive your name, work email address and company, anything you enter in the optional fields, which white paper you ask for, and the page, language and time of your request. For early access we also receive your confirmation that your organisation is registered in the Netherlands. We use these details to answer your request, send you what you asked for, arrange the demo you requested and follow up on your request; for early access, also to contact you when early access opens for your organisation, if that happens within 90 days of our last contact with you. We do not add you to a newsletter. Legal basis: our legitimate interest in handling the requests you send us and following them up.
- **Who processes it.** For the website we use the following parties; section 6 lists those for the service. Resend sends our emails and stores your name and email address from early-access and white-paper requests as a contact, so we can follow up on your request. Resend also emails a copy of every request, including demo requests, to our team's mailbox at our email hosting provider. Vercel

hosts this website; our form handling runs in its Frankfurt region. Cal.com provides the scheduler in step 2 of booking a demo. The scheduler loads only after you submit step 1; at that point we pass your name, email address and the other step-1 details (company, role, number of people you would protect and your message) to Cal.com to pre-fill the booking form, whether or not you then book. Resend, Vercel and Cal.com process this data on our behalf. They are United States companies; transfers outside the EEA rely on the European Commission's standard contractual clauses.

- **Technical logs.** Our host logs each request to this website, including your IP address. Our form handling also logs what you submit, with your IP address and the time, as a backup in case an email does not arrive, and keeps your IP address in memory for ten minutes to limit repeated submissions. We keep these logs for up to 30 days. Legal basis: our legitimate interest in a secure website that does not lose requests.
- **How long we keep your data.** Until you ask us to delete it (privacy@deltawall.ai), but no longer than 90 days after our last contact with you. This period applies to the website data described in this section instead of the periods in section 8; technical logs are kept as stated above.