

Privacyverklaring

Laatst bijgewerkt op 24 september 2026

Deltawall helpt organisaties voorkomen dat gevoelige gegevens in AI-tools terechtkomen. De browserextensie controleert op het apparaat van de medewerker wat die in een AI-tool plakt of uploadt, en maskeert, blokkeert of waarschuwt volgens het beleid van de organisatie. In deze verklaring staat welke persoonsgegevens daarbij worden verwerkt, door wie, waarom en hoe lang.

Het belangrijkste: de tekst die je in een AI-tool typt, de gegevens die worden gemaskeerd en de inhoud en namen van bestanden verlaten je apparaat nooit richting Deltawall. De herkenning gebeurt lokaal in je browser.

1. Wie wij zijn

Deltawall wordt geleverd door Deltawall B.V., ingeschreven bij de Kamer van Koophandel onder nummer 42169421, gevestigd aan De Boelelaan 1095 A, 1081 HV Amsterdam ("wij").

Vragen over privacy of een verzoek over je gegevens: privacy@deltawall.ai. Een beveiligingsprobleem melden: security@deltawall.ai.

2. Onze rol: verwerker of verwerkingsverantwoordelijke

Deltawall wordt afgenomen door organisaties (onze klanten) en gebruikt door hun medewerkers. Wie verantwoordelijk is voor de gegevens, hangt af van om wiens gegevens het gaat:

- **Gegevens van medewerkers** (hun e-mailadres, afdeling, verbonden browsers en de gebeurtenissen die de extensie meldt) verwerken wij **namens de werkgever**. De werkgever is verwerkingsverantwoordelijke en bepaalt het beleid; wij zijn verwerker en handelen volgens een verwerkersovereenkomst met die werkgever. Wil je als medewerker je rechten uitoefenen, wend je dan tot je werkgever. Stuur je je verzoek naar ons, dan sturen we het door en helpen we je werkgever het af te handelen.
- **Gegevens van beheerders** (de mensen die de console van hun organisatie gebruiken), van mensen die zich aanmelden, en de technische gegevens die nodig zijn om de dienst veilig te laten werken, verwerken wij **als verwerkingsverantwoordelijke**.

3. De browserextensie

De extensie werkt alleen op de AI-diensten waarvoor zij toestemming heeft: chatgpt.com, chat.openai.com, claude.ai, gemini.google.com, copilot.microsoft.com, perplexity.ai en chat.deepseek.com. Het herkenningsmodel zit in de extensie zelf en draait op je apparaat; er wordt geen code of model van buitenaf geladen.

Wat je apparaat nooit verlaat: de tekst die je typt of plakt, de waarden die worden herkend en gemaskeerd, en de inhoud en namen van bestanden die je uploadt. Een opgeschoonde kopie van een bestand blijft alleen in het geheugen van de browser en wordt na uiterlijk 15 minuten verwijderd. Wat je

uiteindelijk naar de AI-dienst stuurt, gaat rechtstreeks van jou naar die dienst en niet via Deltawall.

Wat de extensie naar Deltawall stuurt als ze iets herkent (een 'gebeurtenis'):

- welke AI-dienst het betrof (bijvoorbeeld 'chatgpt'), of het om een prompt of een bestand ging, en het tijdstip;
- de soorten gegevens die zijn herkend (bijvoorbeeld 'IBAN' of 'persoonsnaam'), de zekerheid van de herkenning, de regel die gold en wat er gebeurde (gemaskeerd, geblokkeerd, gewaarschuwd, toegestaan);
- gezouten hashes van de herkende waarden: een eenrichtingsberekening met een geheime sleutel per organisatie. De waarde zelf gaat niet mee. Omdat de sleutel bij ons bekend is en korte waarden (zoals een burgerservicenummer) in theorie terug te rekenen zijn, behandelen wij deze hashes als gepseudonimiseerde persoonsgegevens, niet als anonieme gegevens;
- **de reden die je zelf intypt** als je na een waarschuwing toch verstuurt (maximaal 500 tekens). Deze tekst wordt bij de gebeurtenis bewaard en is zichtbaar voor de beheerders van je organisatie. Zet er dus geen gevoelige gegevens in.

Om de extensie te verbinden met je organisatie stuurt ze je werk-e-mailadres (om je een eenmalige code of link te sturen), een eenvoudige omschrijving van de browser (zoals 'Chrome op macOS') en een openbare sleutel. De bijbehorende geheime sleutel blijft in de browser. Daarnaast haalt de extensie regelmatig het beleid van je organisatie op, en meldt ze het ons als ze op een ondersteunde AI-site het invoerveld niet kan vinden (alleen de websitenaam en de dienst), zodat we de extensie kunnen bijwerken.

Wat de extensie op je apparaat bewaart (in de opslag van de browser): de verbinding met je organisatie, het beleid en de sleutel per organisatie voor de hashes, gebeurtenissen die nog verstuurd moeten worden (maximaal 2.000), de laatste 100 verzonden berichten zodat je op de optiepagina kunt zien wat er is verstuurd, tellers van vandaag (die worden niet verstuurd), je taalkeuze en je sleutelpaar. Deze gegevens verdwijnen als je de extensie verwijdt.

Beheert je organisatie de browser centraal (bijvoorbeeld via MDM), dan kan zij de extensie een inschrijvingsleutel en een afdeling meegeven.

4. De console en accounts

Voor de console en de accounts verwerken wij:

Beheerders	naam, werk-e-mailadres, wachtwoord (alleen als versleutelde hash), rol, datum van verificatie en aanmaak
Organisatie	naam en statutaire naam, domein(en), land, sector, omvang, e-mailadres van de functionaris gegevensbescherming, gekozen instellingen
Medewerkers	e-mailadres, naam (als de werkgever die invult), afdeling en groepen, status, verbonden browsers met hun omschrijving en het moment waarop ze het laatst contact hadden
Gebeurtenissen	zie hoofdstuk 3, gekoppeld aan een pseudoniem van de medewerker in plaats van aan zijn naam

Logboek beheerders	welke beheerder wat heeft gedaan (bijvoorbeeld iemand uitgenodigd of een pseudoniem laten herleiden), met de betrokken e-mailadressen of pseudoniemen
E-mail	e-mailadres, onderwerp en inhoud van e-mails die wij versturen (zoals inloglinks en codes), totdat ze verstuurd zijn

Gebeurtenissen worden standaard aan een pseudoniem gekoppeld. Alleen de organisatie kan, via de functies die wij daarvoor bieden, een pseudoniem herleiden tot een persoon; die handeling wordt vastgelegd in het logboek. In de modus 'identiteit in de browser' bewaren wij de koppeling tussen pseudoniem en e-mailadres niet meer zodra de browsers van de medewerker zelf een sleutel hebben (uiterlijk 30 dagen na het inschakelen).

5. Waarom en op welke grondslag

De dienst leveren aan onze klant (herkennen, beleid toepassen, rapporteren)	Voor medewerkersgegevens: in opdracht van de werkgever, volgens de verwerkersovereenkomst. De werkgever bepaalt zelf zijn grondslag (meestal gerechtvaardigd belang of een wettelijke plicht om gegevens te beschermen).
Accounts van beheerders aanmaken en beheren, inloggen	Uitvoering van de overeenkomst met de klant, en ons gerechtvaardigd belang om te weten wie namens een organisatie handelt
Beveiliging, misbruik voorkomen (zoals het beperken van inlogpogingen), storingen oplossen	Gerechtvaardigd belang: een veilige en werkende dienst
De extensie laten blijven werken op AI-sites	Gerechtvaardigd belang; alleen de websitenaam en de dienst, geen inhoud
Wettelijke verplichtingen, zoals de fiscale bewaarplicht voor facturen	Wettelijke verplichting

Wij gebruiken gegevens niet voor advertenties, verkopen ze niet, maken er geen profielen van voor andere doeleinden en gebruiken prompts of gegevens van klanten niet om AI-modellen te trainen.

De extensie past automatisch het beleid van de organisatie toe (maskeren, blokkeren, waarschuwen). Dat is geen besluit dat rechtsgevolgen heeft of je in aanmerkelijke mate treft in de zin van artikel 22 AVG: je kunt je tekst aanpassen en opnieuw versturen, en wat er daarna met gebeurtenissen gebeurt, beslissen mensen binnen je organisatie.

6. Met wie wij gegevens delen

Wij schakelen alleen de volgende subverwerkers in:

Google Cloud (Google Cloud EMEA Ltd., Ierland)	Hosting, database, back-ups, sleutelbeheer. De gegevens staan in de regio europe-west4 (Nederland). Technische logboeken van servers en de load balancer, waarin IP-adressen en soms e-mailadressen kunnen staan, worden door Google verwerkt in een logboekvoorziening die niet aan de EU is gebonden; daarvoor gelden de standaardcontractbepalingen van de Europese Commissie.
---	---

Resend, Inc. (Verenigde Staten)	Versturen van e-mail, zoals inloglinks, codes en uitnodigingen. Resend ontvangt het e-mailadres en de inhoud van de e-mail. Doorgifte buiten de EER gebeurt op basis van de standaardcontractbepalingen van de Europese Commissie.
--	--

Binnen de organisatie van de klant zien beheerders de gegevens die de console toont, volgens de rollen die de klant toekent. Wij geven gegevens verder alleen door als de wet ons daartoe verplicht.

Onze medewerkers bekijken gegevens van klanten niet, tenzij de klant daarom vraagt, het nodig is om een beveiligingsincident of misbruik te onderzoeken, of de wet het vereist.

7. Als je organisatie de AI-gateway gebruikt

Deltawall biedt organisaties optioneel een AI-gateway: een tussenstation voor eigen toepassingen die AI-modellen via een API aanroepen. Alleen in dat geval gaat de inhoud van verzoeken via onze servers naar de AI-aanbieder die de organisatie heeft gekozen (zoals Mistral, Microsoft Azure, OpenAI, Anthropic of DeepSeek). Die aanbieder verwerkt de inhoud volgens zijn eigen voorwaarden en wordt door de organisatie gekozen. De browserextensie gebruikt de gateway niet.

8. Hoe lang wij gegevens bewaren

Gebeurtenissen, logboek beheerders en bewijsrapporten	90 dagen, tenzij de organisatie eerder om verwijdering vraagt. Na het einde van de overeenkomst verwijderen wij ze binnen 90 dagen.
Accounts van beheerders en medewerkers	Zolang de organisatie klant is en het account niet is verwijderd; daarna binnen 90 dagen
Inlogcodes, inloglinks en koppelcodes	Tot ze gebruikt zijn of verlopen (minuten tot uren); daarna binnen 24 uur verwijderd
Inhoud van verzonden e-mails	Direct na verzending gewist; het verzendrecord zelf na 14 dagen
Tellers tegen misbruik (op IP-adres of e-mailadres)	Minuten, tot het tijdvenster verstrijkt
Technische logboeken	Maximaal 30 dagen
Back-ups van de database	Maximaal 14 dagen
Aanmelding die nooit is bevestigd	Tot iemand zich opnieuw aanmeldt met hetzelfde domein, maar maximaal 90 dagen; eerder op verzoek

Facturen en andere gegevens waarvoor een wettelijke bewaarplicht geldt, bewaren wij zo lang als de wet voorschrijft (in Nederland 7 jaar).

9. Beveiliging

Verbindingen zijn versleuteld (TLS). Wachtwoorden worden alleen als hash opgeslagen, inloglinks en codes alleen als hash. De database, back-ups en sleutels staan in een Europese cloudregio. Gebeurtenissen worden in een hashketen vastgelegd zodat achteraf wijzigen opvalt. Toegang binnen ons team is beperkt tot wie die nodig heeft.

10. Cookies

Wij gebruiken alleen functionele cookies van onze eigen website, geen cookies voor analyse, advertenties of volgen. Daarom vragen wij geen toestemming voor cookies.

authjs.session-token, authjs.csrf-token, authjs.callback-url	Ingelogd blijven in de console en inloggen beveiligen; sessie tot 12 uur
dw_employee	Ingelogd blijven op je medewerkerspagina; 12 uur
dw_link, dw_connect, dw_pair_code	Een inloglink, het verbinden van de extensie of een koppelcode afronden; 5 tot 15 minuten
dw_new_gateway_key	Een nieuwe gatewaysleutel eenmalig tonen; 2 minuten
dw-lang	Je taalkeuze onthouden; 1 jaar

11. Je rechten

Je hebt het recht op inzage, correctie, verwijdering, beperking van de verwerking en overdraagbaarheid van je gegevens, en het recht om bezwaar te maken tegen verwerking op grond van gerechtvaardigd belang.

Ben je medewerker van een klant, richt je verzoek dan aan je werkgever (zie hoofdstuk 2). In andere gevallen stuur je je verzoek naar privacy@deltawall.ai. Wij reageren binnen een maand en kunnen je vragen je identiteit te bevestigen.

Ben je het niet eens met hoe wij met je gegevens omgaan, dan kun je een klacht indienen bij de Autoriteit Persoonsgegevens (<https://autoriteitpersoonsgegevens.nl>) of bij de toezichthouder in het land waar je woont of werkt.

12. Chrome Web Store

Het gebruik van informatie die de extensie via Google API's ontvangt, voldoet aan het Chrome Web Store User Data Policy, inclusief de Limited Use-vereisten. Concreet: wij gebruiken gegevens alleen voor het ene doel van de extensie (gevoelige gegevens herkennen en beschermen voordat ze een AI-tool bereiken), dragen ze niet over behalve zoals in deze verklaring staat, laten mensen ze niet inzien behalve in de gevallen in hoofdstuk 6, en verkopen of gebruiken ze nooit voor advertenties, kredietbeoordeling of doorverkoop aan databrokers.

13. Wijzigingen

Wij passen deze verklaring aan als de dienst verandert. Bovenaan staat de datum van de laatste wijziging. Belangrijke wijzigingen melden wij vooraf aan de beheerders van onze klanten.

14. Deze website

Dit hoofdstuk gaat over de openbare website deltawall.ai, niet over de dienst. Voor de website zijn wij verwerkingsverantwoordelijke.

- **Geen cookies van deze website, geen volgtechnieken, geen analyse.** De website deltawall.ai plaatst zelf geen cookies. Met 'onze eigen website' in hoofdstuk 10 bedoelen wij de console op app.deltawall.ai; alleen daar worden die functionele cookies geplaatst. Lettertypen laden wij vanaf

deltawall.ai zelf, niet via een externe dienst. Zodra in stap 2 van het boeken van een demo de planner van Cal.com laadt, of als je die in een nieuw tabblad opent, kunnen Cal.com en zijn beveiligingsdienst Cloudflare eigen cookies plaatsen, zoals de beveiligingscookie __cf_bm.

- **Wat je invult.** Als je early access, een demo of een whitepaper aanvraagt, ontvangen wij je naam, werk-e-mailadres en bedrijf, wat je eventueel invult in de optionele velden, welke whitepaper je aanvraagt, en de pagina, taal en het tijdstip van je aanvraag. Bij early access ontvangen wij ook je bevestiging dat je organisatie in Nederland is ingeschreven. Wij gebruiken deze gegevens om je verzoek te beantwoorden, je toe te sturen wat je hebt aangevraagd, de gevraagde demo in te plannen en je verzoek op te volgen; bij early access ook om contact met je op te nemen zodra early access voor je organisatie opengaat, als dat binnen 90 dagen na ons laatste contact met je gebeurt. Wij zetten je niet op een nieuwsbrief. Grondslag: ons gerechtvaardigd belang om de verzoeken die je ons stuurt af te handelen en op te volgen.
- **Wie het verwerkt.** Voor de website schakelen wij de volgende partijen in; hoofdstuk 6 noemt die voor de dienst. Resend verstuurt onze e-mails en bewaart je naam en e-mailadres uit aanvragen voor early access en whitepapers als contact, zodat wij je aanvraag kunnen opvolgen. Resend stuurt ook een kopie van elke aanvraag, ook van demoaanvragen, naar de mailbox van ons team bij onze e-mailhostingaanbieder. Vercel host deze website; onze formulierverwerking draait in de regio Frankfurt. Cal.com levert de planner in stap 2 van het boeken van een demo. De planner wordt pas geladen nadat je stap 1 hebt verstuurd; op dat moment geven wij je naam, e-mailadres en de andere gegevens uit stap 1 (bedrijf, rol, aantal te beschermen mensen en je bericht) door aan Cal.com om het boekingsformulier vooraf in te vullen, ook als je daarna niet boekt. Resend, Vercel en Cal.com verwerken deze gegevens namens ons. Het zijn Amerikaanse bedrijven; doorgifte buiten de EER gebeurt op basis van de standaardcontractbepalingen van de Europese Commissie.
- **Technische logboeken.** Onze hostingpartij legt elk verzoek aan deze website vast, inclusief je IP-adres. Onze formulierverwerking legt ook vast wat je invult, met je IP-adres en het tijdstip, als reservekopie voor het geval een e-mail niet aankomt, en houdt je IP-adres tien minuten in het geheugen om herhaalde aanvragen te beperken. Deze logboeken bewaren wij maximaal 30 dagen. Grondslag: ons gerechtvaardigd belang bij een veilige website die geen aanvragen kwijtraakt.
- **Hoe lang wij je gegevens bewaren.** Tot je ons vraagt ze te verwijderen (privacy@deltawall.ai), maar uiterlijk 90 dagen na ons laatste contact met je. Deze termijn geldt voor de websitegegevens in dit hoofdstuk, in plaats van de termijnen in hoofdstuk 8; voor technische logboeken geldt de termijn hierboven.