Privacyverklaring

Versie 1.0 - geldig vanaf 31 oktober 2026

Privacyverklaring van Leadhunter B.V. voor haar website en zakelijke dienstverlening.

Wie is verantwoordelijk?

Leadhunter B.V., Goese Dieplaan 97, 4463 LA Goes, KvK 67665284, is verantwoordelijk voor haar eigen website-, contact-, account-, contract-, administratie-, beveiligings- en marketinggegevens. Privacyvragen: info@leadhunter.nl of 088 003 98 88.

Wanneer ons team persoonsgegevens op instructie van een opdrachtgever verwerkt voor onderzoek, zakelijk klantcontact en opvolging, is die opdrachtgever in beginsel verwerkingsverantwoordelijke en Leadhunter verwerker. De concrete rol volgt uit de feitelijke verwerking; deze verklaring of een contractlabel verandert die rol niet.

Welke gegevens verwerken we?

Voor eigen doeleinden: naam, organisatie, functie, zakelijke e-mail, telefoon, account- en toegangsgegevens, correspondentie, factuurgegevens, afspraken, akkoordbewijzen en noodzakelijke technische beveiligingsgegevens.

Bij opdrachten: zakelijke contactgegevens en relevante gespreks- en opvolgingsinformatie volgens de verwerkersovereenkomst. Deze gegevens zijn afkomstig van de opdrachtgever, contactpersonen en relevante openbare zakelijke bronnen binnen de opdracht.

Wij vragen geen gevoelige persoonsgegevens via algemene websiteformulieren. Deel in een digitale websitehulp geen vertrouwelijke of gevoelige informatie. Een zakelijke contactpersoon blijft een natuurlijke persoon; openbare beschikbaarheid betekent niet dat ieder gebruik is toegestaan.

Waarom en op welke grondslag?

Wij behandelen contact- en kennismakingsvragen, bereiden overeenkomsten voor en voeren de samenwerking uit. Waar een persoon zelf partij is kan de grondslag overeenkomst zijn. Bij contactpersonen van een organisatie kan ons gerechtvaardigde belang bij zakelijke communicatie en uitvoering gelden, na afweging van hun belangen.

Facturen en administratie bewaren we vanwege wettelijke verplichtingen. Accounts, fraudepreventie en beveiliging ondersteunen de overeenkomst en ons gerechtvaardigde beveiligingsbelang. Niet-noodzakelijke websiteanalyse gebeurt op toestemming.

Voor marketing gebruiken we alleen een passende grondslag én voldoen we aan toepasselijke kanaalregels. Waar toestemming vereist is, vragen en registreren we die afzonderlijk. Een algemene aanmelding of eerder klantcontact geldt niet automatisch als toestemming voor iedere vorm van marketing.

Bewaartermijnen

Contact- en kennismakingsgegevens: als voorgesteld uitgangspunt tot 24 maanden na het laatste relevante contact, tenzij eerder verwijderen passend is of een lopende afspraak of geschil bewaring vereist.

Financiële administratie: in beginsel zeven jaar voor zover de wettelijke bewaarplicht dat vereist. Bewijs van contractuele acceptatie: zolang noodzakelijk voor uitvoering en onderbouwing van rechten, met een gemotiveerde retentie.

Account- en beveiligingsgegevens: zolang noodzakelijk voor toegang, onderzoek en beveiliging, volgens vast te stellen concrete retentie. We nemen geen automatische dertig-dagen-SaaS-archiefcyclus over voor de bestaande klantportal.

Gegevens namens opdrachtgevers: volgens hun instructie en de verwerkersovereenkomst. Bezwaar- en afmeldgegevens blijven zo nodig minimaal bewaard om ongewenste herhaling te voorkomen.

GA4: voor de bestaande LH-property is in Radar een bewaartermijn van veertien maanden als eerdere instelling vastgelegd; vóór livegang wordt deze instelling in Analytics opnieuw gecontroleerd. Wij bewaren niet langer dan noodzakelijk.

Persoonlijk klantcontact namens een opdrachtgever

Ons team kan zakelijke contactpersonen namens een opdrachtgever benaderen. Daarbij volgen we de afgesproken doelgroep en houden we rekening met toepasselijke regels, rechtsvorm, kanaal en land. U mag vragen namens welke organisatie wij contact leggen.

Wilt u niet meer voor direct marketing worden benaderd? Geef dat direct aan of mail info@leadhunter.nl. Wij verwerken het bezwaar en stemmen de noodzakelijke blokkade met de betreffende opdrachtgever af. Een verzoek over overige klantgegevens leiden we naar de verantwoordelijke opdrachtgever.

Websiteanalyse en cookie-instellingen

Na uw toestemming gebruiken wij Google Analytics 4 om bezoek aan deze website en gebruik van contact- en boekingsknoppen te meten. Google ontvangt daarbij technische browser- en verbindingsinformatie, pagina-adressen zonder URL-queryparameters en meetgebeurtenissen. De LH-meetcode stuurt geen ingevulde namen, e-mailadressen, telefoonnummers, account-ID’s, wachtwoorden of chatinhoud mee. Google Signals en advertentiepersonalisatie staan in de meetcode uit.

De rapportages helpen Leadhunter beoordelen welke informatie en contactmogelijkheden worden gebruikt. Bevoegde beheerders kunnen de eigen websitegegevens bekijken. Wanneer de koppeling met Radar is geactiveerd, kunnen rapportgegevens, zoals geaggregeerde bezoekcijfers, zoekopdrachten en pagina-informatie uit Search Console, worden gebruikt voor bedrijfsinzichten en voorstellen voor websiteverbetering. Andere Radar-bedrijven krijgen geen toegang tot deze LH-gegevens.

De publieke LH-website vraagt bezoekers geen toegang tot hun Google-account, Google Analytics of Search Console. Het koppelen van Leadhunters eigen Google-properties aan Radar is een afzonderlijke beheerdershandeling. De website krijgt geen OAuth-tokens van bezoekers.

Toestemming voor niet-noodzakelijke meting staat los van aanmelding en voorwaarden. Via Cookie-instellingen op de voorwaardenpagina kunt u toestaan, weigeren of uw voorkeur intrekken. In de offline ontwerpversie blijft alle meting uit.

Botcontrole bij aanmelding

Voor bescherming tegen geautomatiseerde aanmeldingen wordt Cloudflare Turnstile voorbereid. De beveiligingscontrole verwerkt technische browser- en verbindingsgegevens. We sturen naam, e-mail en wachtwoord niet als invoervelden naar de botcontrole.

De websitebackend moet het controletoken verifiëren voordat zij een aanmelding doorgeeft. Cloudflare heeft eigen privacy-informatie. De feitelijke productinstellingen en relevante leveranciersrol worden vóór activering gecontroleerd.

Digitale wegwijzer en eventuele AI

Zolang AI uitgeschakeld is, zoekt de digitale wegwijzer lokaal in vaste website-informatie. Uw zoekvraag blijft dan in uw browser en gaat niet naar een AI-provider.

Wanneer de AI-assistent wordt geactiveerd en als zodanig herkenbaar is, verwerkt OpenAI via de API uw vraag, een beperkt aantal recente berichten uit dit gesprek en relevante goedgekeurde bedrijfsinformatie om een antwoord te geven. De aanvraag gebruikt store=false. Dat is geen belofte dat de provider onder alle omstandigheden geen technische of veiligheidsretentie heeft. Deel geen gevoelige of vertrouwelijke klantinformatie.

De website slaat geen vrije chattekst op in de LH-database. Supabase verwerkt de serveraanroep, goedgekeurde kennis en beperkte beveiligings- en gebruiksregistratie. Voor misbruikbeperking wordt een afgeleide IP-code gebruikt; deze wordt na twee dagen uit de AI-gebruiksregistratie verwijderd. Technische platformlogs kunnen een afzonderlijke bewaartermijn hebben, die vóór activering wordt gecontroleerd.

Voor analyses binnen Radar kunnen relevante LH-rapportgegevens en bedrijfscontext via de API met OpenAI worden verwerkt. Google-OAuth-tokens worden niet aan OpenAI meegestuurd. Deze functie geeft geen toegang tot gegevens van andere opdrachtgevers en publiceert geen nieuwe teksten zonder de afgesproken goedkeuring.

De AI-chat wordt pas geactiveerd nadat de gegevensstromen en privacy-informatie zijn gecontroleerd. Binnen opdrachten worden eventuele aanvullende AI-verwerkingen eerst afzonderlijk vastgelegd. Er is geen algemene toestemming om klantbestanden of gespreksnotities voor andere opdrachtgevers of algemene modeltraining te gebruiken.

Ontvangers en internationale verwerking

Gegevens kunnen waar noodzakelijk worden verwerkt door bevoegde medewerkers, zelfstandig ingeschakelde uitvoerders en leveranciers voor hosting, communicatie, beveiliging, administratie of analyse. Alleen passende noodzakelijke toegang wordt verleend.

Wij delen gegevens met een opdrachtgever voor wie we de opdracht uitvoeren en met bevoegde adviseurs of instanties wanneer dat noodzakelijk of wettelijk verplicht is. We verkopen geen persoonsgegevens.

Bij diensten buiten de EER gelden de vereiste doorgiftewaarborgen, zoals een toepasselijk adequaatheidsbesluit of standaardcontractbepalingen, en waar nodig aanvullende maatregelen. De feitelijke rol en afspraken worden per gegevensstroom beoordeeld. De technische leveranciers van de nieuwe website zijn niet automatisch dezelfde als die van de bestaande klantportal of telefoonsystemen.

Een kennismaking boeken

Voor een kennismaking verwerken wij uw naam, bedrijfsnaam, e-mailadres, telefoonnummer, gekozen datum en tijd en uw voorkeur voor telefonisch contact of beeldbellen. Wij gebruiken deze gegevens om de afspraak vast te leggen, voor te bereiden en hierover contact op te nemen.

De beschikbare tijdvakken worden door Leadhunter bepaald. De website leest geen privéagenda van Susan, Anton of een bezoeker uit. Een gekozen tijd wordt in onze beveiligde website-backend vastgelegd; dubbele boekingen worden gecontroleerd.

De klant en de betrokken medewerker ontvangen een bevestiging met agenda-uitnodiging via e-mail. Het toevoegen daarvan aan een eigen agenda valt onder de gebruikte agenda- en maildienst. Voor een wijziging of annulering kunt u antwoorden op de bevestigingsmail aan info@leadhunter.nl.

De digitale assistent kan geen afspraken maken of uw agenda beheren. Bij beeldbellen kunnen de verbindingsgegevens afzonderlijk door Leadhunter worden verstrekt.

Sociale media en externe websites

Links naar LinkedIn en later bevestigde Facebook- en Instagramaccounts openen externe websites. Alleen door zo’n link op te nemen laden we geen sociale trackingpixel of ingesloten tijdlijn.

Bij contact of bezoek op een sociaal platform gelden ook de eigen privacyregels van dat platform. Toekomstige publicatie via gekoppelde hulpmiddelen wordt apart ingericht; een footerlink is geen actieve accountkoppeling.

LinkedIn en eigen marketing via Radar

Een link naar LinkedIn geeft Leadhunter geen toegang tot het LinkedIn-account van een bezoeker. De publieke website vraagt bezoekers geen LinkedIn-OAuth-toestemming en haalt via zo’n link geen profiel-, connectie- of berichtgegevens op.

Wanneer een bevoegde beheerder Leadhunters eigen pagina aan Radar koppelt, kan Radar met de verleende rechten de eigen publicaties en geaggregeerde paginastatistieken verwerken en goedgekeurde teksten publiceren. Daarvoor geldt ook de specifieke Radar-privacyinformatie. Een gewone websitebezoeker wordt hierdoor niet zelf aan Radar gekoppeld.

Via de LinkedIn-API opgehaalde brongegevens worden in de huidige Radar-inrichting niet aan Maya/OpenAI als AI-invoer doorgegeven. Eigen, onafhankelijk aangeleverde bedrijfsinformatie en website-inhoud kunnen wel worden gebruikt voor contentvoorstellen. Publicatie volgt het afgesproken goedkeuringsproces.

LinkedIn-ledengegevens worden niet via deze koppeling gebruikt voor Leadhunters prospectlijsten of CRM-verrijking. Het gebruik voor paginabeheer geeft geen toestemming voor acquisitie. Voor privacyvragen of een verwijderverzoek: info@leadhunter.nl. Voor contact of bezoek op LinkedIn gelden daarnaast de privacyregels van LinkedIn.

Bescherming van gegevens en Google-rapporten

Voor de nieuwe website worden beveiligde HTTPS/TLS-verbindingen, taakgebonden toegang, server-side secretbeheer en controles op toegangsrechten toegepast voor zover de betreffende functie is geactiveerd. De feitelijke instellingen worden vóór livegang gecontroleerd. Wij vragen geen bijzondere persoonsgegevens via algemene formulieren en gebruiken geen bezoekerstoegang tot Google-accounts.

Wanneer een bevoegde beheerder Leadhunters eigen Analytics- of Search Console-property in Radar koppelt, beschermt Radar de rapporten met server- en databaseautorisatie per bedrijf. OAuth-tokens worden aanvullend met AES-256-GCM versleuteld en aan bedrijf en gebruiker gebonden; secrets blijven server-side. De primaire Radar-database staat in Frankfurt en gebruikt versleutelde opslag. Gegevensoverdracht gebruikt HTTPS/TLS. Alleen noodzakelijke leestoestemming wordt gevraagd. Voor deze afzonderlijke beheerderskoppeling geldt tevens de Radar-privacyverklaring op https://www.bizzi-b-radar.com/privacy.html.

Deze bescherming beschrijft geen bezoekers-OAuth-koppeling en verleent geen algemene toegang tot gegevens van opdrachtgevers. Menselijke toegang is beperkt tot bevoegde personen en noodzakelijke uitvoering, ondersteuning, beveiliging of wettelijke verplichtingen. Geen enkele beveiligingsmaatregel biedt absolute veiligheid. Vragen, incidenten of verzoeken over Leadhunters eigen verwerking: info@leadhunter.nl.

Automatische publicatiecontrole bij eigen marketing via Radar

Wanneer Leadhunter via Radar eigen artikelen of sociale posts publiceert, controleert Radar de uitgaande tekst en het beeld automatisch met AI, voor LinkedIn, Facebook, Instagram en gekoppelde websites voor zover de koppeling is vrijgegeven. Bij die automatische controle kijkt geen medewerker van Radar mee; dit betekent niet dat Leadhunters eigen team geen eigen content voorbereidt of beoordeelt.

Een blokkering verhindert publicatie via Radar; een waarschuwing vraagt een afzonderlijke bevestiging. De gebruiker kan wijzigen of zelf buiten Radar publiceren, onder eigen verantwoordelijkheid en volgens wet- en platformregels. De controle is geen garantie op juistheid, rechtmatigheid of rechtenvrijheid. OpenAI verwerkt de uitgaande inhoud volgens Radars privacy-informatie. Via de LinkedIn-API opgehaalde brongegevens worden niet voor deze controle doorgegeven.

Radar bewaart beperkte controleresultaten 24 uur en ontdubbelde beveiligingstellingen per bedrijf/gebruiker 30 dagen, met opruiming ieder kwartier. Radar Beheer toont aantallen en percentages, geen publicatie-inhoud of afkeurreden. Deze websitebezoeker wordt door Leadhunters eigen publicatieproces niet zelf aan Radar gekoppeld. Een eventuele inzet van deze werkwijze voor content namens een opdrachtgever wordt vooraf binnen die opdracht en de toepasselijke privacyafspraken vastgelegd.

Beveiliging en uw rechten

Wij treffen passende technische en organisatorische maatregelen, waaronder taakgebonden toegang, vertrouwelijkheid en beveiligde gegevensoverdracht. Geen beveiliging kan absolute bescherming garanderen.

U kunt vragen om inzage, correctie, verwijdering, beperking en waar toepasselijk overdraagbaarheid. U kunt toestemming intrekken en bezwaar maken, in het bijzonder tegen direct marketing. We controleren uw identiteit passend en reageren in beginsel binnen één maand, met de wettelijke mogelijkheden voor verlenging.

Voor eigen verwerkingen bereikt u ons via info@leadhunter.nl. Voor gegevens die wij namens een opdrachtgever verwerken, verwijzen of ondersteunen we uw verzoek richting die opdrachtgever. U kunt een klacht indienen bij de Autoriteit Persoonsgegevens.

Wij gebruiken de hier beschreven verwerking niet voor uitsluitend geautomatiseerde beslissingen met rechtsgevolgen of vergelijkbare aanzienlijke gevolgen. Bij wijzigingen publiceren we een actuele versie; nieuwe doeleinden of vereiste toestemming worden niet alleen via een tekstwijziging ingevoerd.