HAGE HOSTING

Privacyverklaring

Hoe wij omgaan met jouw persoonsgegevens bij onze website en dienstverlening.

Versie 25 oktober 2026

1. Wie zijn wij?

Hage Hosting respecteert je privacy. In deze verklaring leggen wij uit welke persoonsgegevens wij verwerken, waarom wij dat doen, met wie wij gegevens delen en welke rechten je hebt.

Hage Hosting
Adres: Oude Moolweg 3
4325 EA Renesse, Nederland
Telefoon: 0111-202088
Website: https://hagehosting.com
Algemeen e-mailadres: info@hagehosting.com
Privacyvragen en verzoeken: support@hagehosting.com
Contactpersoon voor privacy: Sander Hage
KvK-nummer: 86151762

Hage Hosting is verwerkingsverantwoordelijke voor de persoonsgegevens die wij voor onze eigen bedrijfsvoering verwerken, zoals klantbeheer, facturatie, ondersteuning en de beveiliging van onze dienstverlening. Voor gegevens die wij uitsluitend in opdracht van klanten hosten of beheren, geldt de toelichting in onderdeel 3.

2. Voor welke diensten geldt deze verklaring?

Deze verklaring heeft betrekking op onze website, het klantenportaal, contactformulieren, offertes, bestellingen, ondersteuning en de levering en het beheer van:

- domeinnamen en DNS-diensten;
- DirectAdmin- en Plesk-webhosting, websites, databases en e-mail;
- Flex Cloud VPS met gedeelde CPU en Dedicated Cloud VPS met dedicated CPU;
- fysieke dedicated servers;
- Microsoft-, Office- en zakelijke e-mailproducten;
- DirectAdmin-, Plesk- en andere bij de dienst bestelde softwarelicenties;
- SSL/TLS-certificaten;
- back-ups, opslag, migraties, beveiliging en aanvullend beheer, voor zover overeengekomen.

Welke gegevens nodig zijn, hangt af van de dienst die je gebruikt. De privacyregels van zelfstandige leveranciers kunnen daarnaast gelden voor hun eigen verwerkingen. Wij blijven verantwoordelijk voor onze eigen keuzes en verplichtingen.

3. Onze rol bij jouw klantgegevens

Bij hosting en beheer kunnen wij persoonsgegevens verwerken die jij in websites, databases, mailboxen, servers of back-ups opslaat. Als jij het doel en de middelen van die verwerking bepaalt, ben jij doorgaans verwerkingsverantwoordelijke en verwerken wij deze gegevens als verwerker. Ben jij zelf verwerker voor een opdrachtgever, dan kunnen wij subverwerker zijn.

Voor deze dienstverlening leggen wij de afspraken vast in een verwerkersovereenkomst. Daarin staan onder meer de instructies, beveiliging, inzet van subverwerkers, incidentmelding, ondersteuning bij privacyverzoeken en het teruggeven of verwijderen van gegevens.

Wij gebruiken de inhoud van jouw gehoste gegevens niet voor eigen reclame. Toegang tot die inhoud beperken wij tot wat noodzakelijk is voor de opdracht, geautoriseerde ondersteuning, herstel, beveiliging of een toepasselijke wettelijke verplichting. Als wij gegevens voor een eigen beveiligingsdoel verwerken, beoordelen wij daarvoor afzonderlijk onze rol, noodzaak en grondslag.

4. Welke persoonsgegevens verwerken wij?

Wij verwerken, afhankelijk van de dienst:

a. Contact- en klantgegevens

Naam, bedrijfsnaam, contactpersoon, adres, telefoonnummer, e-mailadres, klantnummer en, indien relevant, KvK- en btw-gegevens. Zakelijke gegevens zijn persoonsgegevens voor zover zij op een persoon betrekking hebben.

b. Account- en bestelgegevens

Accountnaam, authenticatiegegevens, toegangsrechten, bestellingen, gekozen producten en instellingen, contracten, verlengingen en opzeggingen. Wij behandelen wachtwoorden en toegangssleutels met passende technische bescherming.

c. Administratieve gegevens

Factuurgegevens, betaalstatus, transactiegegevens, bankrekeningnummer indien nodig voor de betaling, en correspondentie over betalingen. Welke betaalgegevens wij ontvangen, hangt af van de betaalmethode en betaaldienstverlener.

d. Domein-, certificaat- en licentiegegevens

Domeinnaam, houder- en contactgegevens, registratie- en wijzigingsgegevens, verificatieresultaten, certificaatgegevens, licentie-identificatie en IP-adres of serverkenmerk waaraan een licentie is gekoppeld. Voor sommige domeinextensies of specifieke verificatieprocedures kunnen daarnaast noodzakelijke identiteitsgegevens worden verwerkt, zoals een paspoort- of ID-documentnummer en, uitsluitend wanneer nodig en rechtmatig, een afgeschermde kopie van een identiteitsbewijs. Dit geldt niet voor alle domeinregistraties. Zie onderdeel 6.

e. Technische en beveiligingsgegevens

IP-adres, tijdstip, browser- en apparaatgegevens, inlogpogingen, server- en toegangslogs, foutmeldingen, e-mailmetadata en signalen over malware, spam, fraude of ander misbruik. Verbruiksgegevens kunnen onder meer gebruiksduur, opslag en dataverkeer omvatten voor beheer en facturatie.

f. Communicatie en ondersteuning

Berichten, supporttickets, bijlagen en gegevens die je verstrekt voor het onderzoeken of oplossen van een probleem. Verstrek geen wachtwoorden, identiteitsdocumenten of andere gevoelige gegevens via gewone e-mail of een openbaar formulier als dat niet nodig is.

g. Gehoste inhoud

Bestanden, databases, e-mailberichten, back-ups en migratiegegevens die wij in jouw opdracht verwerken. De aard van deze gegevens wordt in belangrijke mate bepaald door jou en je gebruikers.

Wij ontvangen gegevens van jou, bevoegde contactpersonen en gebruikers, technische systemen en, waar nodig, betaal-, registratie-, certificaat-, licentie- en infrastructuurpartners.

5. Waarom verwerken wij gegevens en op welke grondslag?

- Offertes en dienstverlening: voor het behandelen van een aanvraag en het leveren, beheren, wijzigen en beëindigen van de bestelde diensten. Grondslag: uitvoering van een overeenkomst of stappen op jouw verzoek voorafgaand daaraan. Voor contactpersonen van zakelijke klanten kan het gerechtvaardigd belang gelden om de zakelijke relatie te onderhouden.
- Accountbeheer, ondersteuning en migratie: voor toegang tot diensten, het beantwoorden van vragen en het uitvoeren van overeengekomen werkzaamheden. Grondslag: uitvoering van de overeenkomst of het gerechtvaardigd belang bij goede zakelijke dienstverlening. Voor gehoste klantdata gelden daarnaast de instructies uit de verwerkersovereenkomst.
- Facturatie en betaling: voor het berekenen en innen van kosten en het bijhouden van de administratie. Grondslag: uitvoering van de overeenkomst en wettelijke fiscale verplichtingen. Voor noodzakelijk incassobeheer kan het gerechtvaardigd belang bij betaling van vorderingen gelden.
- Domeinregistratie, certificaten en licenties: voor aanvraag, uitgifte, verificatie, verlenging en beheer. Grondslag: uitvoering van de overeenkomst en, voor zover van toepassing, concrete wettelijke verplichtingen. Een leveranciersvoorwaarde is op zichzelf geen wettelijke verplichting.
- Beveiliging en continuïteit: voor het voorkomen, herkennen, onderzoeken en beperken van ongeoorloofde toegang, malware, spam, fraude en verstoringen. Grondslag: ons gerechtvaardigd belang en dat van klanten bij veilige, betrouwbare systemen, en toepasselijke wettelijke verplichtingen. Wij wegen deze belangen af tegen jouw privacy en beperken de verwerking tot wat noodzakelijk is.
- Wettelijke verzoeken en incidentmeldingen: voor het voldoen aan toepasselijke wettelijke verplichtingen en rechtmatige vorderingen van bevoegde autoriteiten. Wij beoordelen de bevoegdheid, rechtsgrond en reikwijdte voordat wij gegevens verstrekken, voor zover de wet dat toestaat.
- Dienstberichten: voor informatie over onderhoud, beveiliging, betalingen, contracten en wijzigingen die voor jouw dienst relevant zijn. Grondslag: uitvoering van de overeenkomst, gerechtvaardigd belang of een toepasselijke wettelijke verplichting.
- Marketing en niet-noodzakelijke metingen: alleen als wij deze toepassen en daarvoor een geldige grondslag hebben. Waar toestemming nodig is, vragen wij die vooraf. Voor commerciële e-mail houden wij ook rekening met de regels voor elektronische communicatie. Je kunt je eenvoudig afmelden en bezwaar maken tegen direct marketing.

Gegevens die nodig zijn voor een bestelling, betaling of verplichte verificatie zijn noodzakelijk om de betreffende dienst te kunnen leveren. Ontbreken deze, dan kunnen wij de aanvraag mogelijk niet uitvoeren. Optionele gegevens hoef je niet te verstrekken.

6. Domeinnaamgegevens en verificatie

Voor het registreren en beheren van domeinnamen verstrekken wij noodzakelijke gegevens aan de betrokken registrar en registry. Waar de wet dit vereist, verzamelen en controleren wij registratiegegevens, houden wij deze actueel en behandelen wij rechtmatige verzoeken om toegang tot niet-openbare registratiegegevens.

Je kunt daarom een verzoek ontvangen om contactgegevens te bevestigen of te corrigeren. Niet iedere registratie vraagt om een identiteitsbewijs. Voor bepaalde extensies of bij een gerichte controle kan de registrar of registry aanvullende identiteitsgegevens of een kopie van een geldig identiteitsbewijs vragen. Een documentnummer is iets anders dan een kopie van het document: wij vragen niet meer dan de betreffende rechtmatige procedure noodzakelijk maakt.

Doel en grondslag

Aanvullende identificatie kan nodig zijn om de identiteit of bevoegdheid van de domeinhouder vast te stellen, registratiegegevens te controleren of fraude en onrechtmatige wijzigingen te voorkomen. Vóór het opvragen van een document informeren wij je over de concrete reden, de benodigde gegevens, de ontvanger en de bewaartermijn of de criteria daarvoor.

De grondslag hangt af van de concrete verwerking. Alleen waar een voor ons geldende wettelijke verplichting bestaat, beroepen wij ons daarop. Voor objectief noodzakelijke verwerking voor jouw domeinaanvraag kan uitvoering van de overeenkomst gelden. Voor aanvullende fraudepreventie kan een gerechtvaardigd belang gelden, na beoordeling van de noodzaak, minder ingrijpende alternatieven en jouw privacybelangen. Een eis van een registrar of registry is op zichzelf geen wettelijke verplichting en rechtvaardigt niet automatisch een volledige ID-kopie.

Welke gegevens moeten zichtbaar zijn?

Dit verschilt per domeinextensie en verificatieprocedure. Wij geven vooraf aan welke gegevens nodig zijn. Maak je BSN en andere niet-noodzakelijke gegevens onleesbaar, ook op de achterzijde en waar deze in de machineleesbare strook (MRZ) voorkomen. Een pasfoto scherm je af, tenzij de rechtmatige verificatiemethode aantoonbaar vereist dat deze zichtbaar is. Een BSN wordt alleen verwerkt als daarvoor een specifieke wettelijke bevoegdheid bestaat. Een paspoort- of documentnummer vragen wij alleen als dit voor de betreffende procedure noodzakelijk en rechtmatig is; anders scherm je dit eveneens af.

Je kunt de KopieID-app van de Rijksoverheid gebruiken om gegevens af te schermen en een watermerk met datum, doel en ontvanger toe te voegen. Wanneer de ontvangende partij een bewerking niet accepteert, beoordelen wij eerst de noodzaak en rechtmatigheid van dat verzoek; wij vragen niet zonder meer om een onbewerkte kopie.

Aanlevering en ontvangers

Waar mogelijk laat je de verificatie rechtstreeks uitvoeren via de beveiligde verificatievoorziening van de registrar of registry. Als Hage Hosting een document zelf moet ontvangen en doorgeven, gebeurt dat via een daarvoor aangewezen beveiligde route, met beperkte toegang en alleen aan de partij die de verificatie moet uitvoeren. Stuur geen identiteitsdocument ongevraagd als gewone e-mailbijlage of als regulier supportticket. Wij geven je instructies voor de betreffende procedure.

Bewaring van kopieën en verificatiegegevens

Een kopie die Hage Hosting ontvangt, gebruiken wij uitsluitend voor de betreffende verificatie. Wij verwijderen onze werk- en uploadkopieën zodra de procedure is afgerond of beëindigd en de kopie niet meer noodzakelijk is. Een langere bewaring moet een afzonderlijke aantoonbare rechtsgrond en noodzakelijke termijn hebben; daarover informeren wij je. Een documentnummer of beknopte registratie van het verificatieresultaat kan nog nodig zijn voor de domeinregistratie, ook nadat de kopie is verwijderd. Ook daarvoor geldt een afzonderlijk onderbouwde bewaartermijn.

De algemene termijn van 180 dagen voor logbestanden geldt niet voor de inhoud van identiteitsdocumenten. Als een document in een back-up terechtkomt, geldt de afzonderlijke retentie uit onderdeel 9; de actieve verwijdering betekent dan niet dat iedere back-upkopie onmiddellijk is gewist. Wij richten de verwerking zo in dat onnodige duplicaten en opname in reguliere back-ups worden beperkt.

Als de registrar of registry het document zelf ontvangt of als zelfstandig verwerkingsverantwoordelijke bewaart, gelden voor die verwerking de door die partij toegelichte doeleinden en bewaartermijnen. Wij informeren je wie de ontvanger is en waar je die informatie kunt vinden. Wij kunnen niet namens een zelfstandige ontvanger beloven dat zijn kopie binnen 48 of 72 uur wordt verwijderd. Onze eigen verplichtingen bij het verzamelen en verstrekken blijven gelden.

Welke registratiegegevens via een register, WHOIS- of RDAP-dienst openbaar zijn, hangt af van het domein, de toepasselijke regels en het soort gegevens. Een registratie betekent niet dat alle persoonsgegevens openbaar mogen worden gemaakt. Over de verwerking bij de registrar en registry informeren deze partijen ook via hun eigen privacyinformatie.

7. Met wie delen wij gegevens?

Wij delen alleen gegevens die nodig zijn voor een omschreven doel, met passende afspraken en een geldige grondslag. Afhankelijk van je dienst kunnen ontvangers zijn:

- infrastructuur-, datacenter-, cloud- en back-upleveranciers;
- domeinregistrars, registries en DNS-partners;
- certificaatautoriteiten en leveranciers van software, licenties en Microsoft-diensten;
- betaaldienstverleners, banken en aanbieders van administratie- of boekhoudsoftware;
- leveranciers van klantenportaal-, support-, e-mail- en beveiligingssystemen;
- professionele adviseurs of incassodienstverleners wanneer dit noodzakelijk is;
- bevoegde autoriteiten, toezichthouders en incidentresponsorganisaties wanneer een rechtmatige verplichting of andere geldige grondslag dit rechtvaardigt.

De Cloud VPS-dienst maakt gebruik van infrastructuur van Hetzner. Voor het contactformulier gebruikt onze website hCaptcha van Intuition Machines; zie onderdeel 10.

Met partijen die namens ons persoonsgegevens verwerken, sluiten wij waar vereist een verwerkersovereenkomst. Sommige ontvangers verwerken gegevens voor eigen wettelijke of zakelijke doeleinden en zijn daarvoor zelfstandig verwerkingsverantwoordelijke. Voor gehoste klantdata gelden bovendien de subverwerkersafspraken met de klant.

Je kunt via support@hagehosting.com informatie opvragen over de ontvangers en subverwerkers die voor jouw dienst worden ingezet, hun rol, verwerkingslanden en toepasselijke waarborgen. Bij een verzoek om identificatie noemen wij de betrokken registrar of registry vooraf.

8. Verwerking binnen en buiten Europa

De opslag van gegevens op de door Hage Hosting gebruikte servers vindt plaats in Duitsland, binnen de Europese Unie en de Europese Economische Ruimte (EER). Dit betreft onze serveropslag; het betekent niet automatisch dat iedere externe leverancier alle gegevens uitsluitend in Duitsland verwerkt. Voor onder meer domeinregistraties, Microsoft-producten, betaalverwerking, licenties en formulierbeveiliging kunnen andere ontvangers en verwerkingslanden betrokken zijn. Ook toegang vanuit een land buiten de EER kan een internationale doorgifte vormen.

Voor doorgifte buiten de Europese Economische Ruimte (EER) is een geldige doorgifteregeling nodig. Afhankelijk van de ontvanger kan dat een toepasselijk adequaatheidsbesluit van de Europese Commissie zijn of passende waarborgen, zoals de Europese standaardcontractbepalingen. Waar nodig beoordelen wij aanvullende risico's en nemen wij aanvullende maatregelen.

Via support@hagehosting.com kun je informatie opvragen over de concrete ontvangers, verwerkingslanden en toepasselijke doorgifteregeling, en waar van toepassing een kopie van de waarborgen ontvangen. Daarbij kunnen vertrouwelijke gegevens worden afgeschermd.

9. Hoe lang bewaren wij gegevens?

Wij bewaren gegevens niet langer dan nodig voor hun doel. Daarna verwijderen of anonimiseren wij ze, tenzij een wettelijke verplichting of een aantoonbare noodzaak voor een concrete vordering of procedure langer bewaren rechtvaardigt. Gegevens die voor meerdere doelen worden gebruikt, beoordelen wij per doel.

De volgende termijnen vormen ons bewaarbeleid:

- Fiscale basisadministratie en factuurgegevens: in beginsel zeven jaar volgens de fiscale bewaarplicht. Voor gegevens waarvoor een langere wettelijke termijn geldt, geldt die termijn. Niet alle gegevens uit een klantaccount vallen automatisch onder deze bewaarplicht.
- Klant- en contractgegevens: gedurende de dienstverlening en daarna voor zover nodig voor de eindafrekening, afhandeling van openstaande verplichtingen of een concreet geschil. Na afloop van die doelen verwijderen of anonimiseren wij gegevens die niet onder een afzonderlijke bewaarplicht vallen.
- Aanvragen zonder overeenkomst: gedurende de behandeling van de aanvraag en de daarop aansluitende correspondentie. Wanneer duidelijk is dat geen overeenkomst tot stand komt en verdere opvolging niet nodig is, verwijderen wij de gegevens, tenzij een concreet geschil of andere aantoonbare grondslag bewaring noodzakelijk maakt.
- Supporttickets en correspondentie: gedurende de afhandeling en daarna zolang de inhoud nodig is voor het beheer van de betreffende dienst, de opvolging van het gemelde probleem of de afhandeling van een concrete aanspraak. De noodzaak hangt af van het onderwerp en de lopende klantrelatie. Tijdelijke toegangscodes en onnodige gevoelige bijlagen verwijderen wij zodra deze niet meer nodig zijn.
- Reguliere toegangs-, fout- en beveiligingslogs: 180 dagen na vastlegging. Wij gebruiken deze gegevens voor technisch beheer, het onderzoeken van storingen en het voorkomen en onderzoeken van beveiligingsincidenten en misbruik. Na deze termijn worden zij verwijderd of onomkeerbaar geanonimiseerd. Alleen gegevens die aantoonbaar nodig zijn voor een concreet incident, een geschil of een toepasselijke wettelijke verplichting kunnen afzonderlijk langer worden bewaard; de reden, selectie, bewaartermijn en toegang worden vastgelegd. Deze termijn geldt voor logs die wij voor onze eigen dienstverlening beheren. Voor logs die klanten zelfstandig binnen hun VPS of applicatie beheren, bepaalt de verantwoordelijke klant een passende termijn.

- ID-kopieën bij domeinverificatie: alleen zolang noodzakelijk voor de concrete verificatie, met verwijdering van onze actieve kopieën zodra de procedure is afgerond of beëindigd en de kopie niet meer nodig is. Eventuele afzonderlijk noodzakelijke documentnummers en verificatieresultaten worden niet automatisch tegelijk met de kopie verwijderd. Vóór verzameling informeren wij je over de specifieke bewaartermijn of de criteria daarvoor en de betrokken ontvanger; zie onderdeel 6.
- Gehoste inhoud na beëindiging: teruggeven of verwijderen volgens de verwerkersovereenkomst en de afgesproken export- en verwijdertermijnen. Een fiscale bewaarplicht voor onze facturen is geen reden om jouw volledige mailbox of database te bewaren.
- Back-ups van de betreffende shared-hostingpakketten: externe back-upretentie van 60 dagen en een complete back-up die maximaal zeven dagen beschikbaar is, overeenkomstig de productomschrijving. Voor VPS, fysieke servers en andere opslag gelden de afzonderlijk bestelde back-upafspraken. Dit is geen algemene toezegging dat alle diensten automatisch een back-up hebben.
- Sessiecookies en voorkeuren: zolang nodig voor de sessie of de gekozen instelling. Toestemmingsregistraties bewaren wij zolang nodig om de geldende keuze te respecteren en de rechtmatigheid daarvan aan te tonen. Voor verificatiegegevens gelden het concrete verificatiedoel en de informatie die wij vooraf bij de betreffende procedure verstrekken.

Na verwijdering uit actieve systemen kunnen gegevens nog tijdelijk in beveiligde back-ups voorkomen totdat deze volgens hun retentie worden overschreven of verwijderd. Wij gebruiken die kopieën alleen voor noodzakelijk herstel en beveiliging. Bij herstel voeren wij eerdere geldige verwijderingen opnieuw uit waar nodig. Uitzonderingen op normale verwijdering worden beperkt en gedocumenteerd.

10. Cookies, metingen en bescherming van formulieren

Wij gebruiken technisch noodzakelijke functies voor onder meer sessies, inloggen, het bestelproces en beveiliging. Voor cookies die strikt noodzakelijk zijn en voor analytische cookies die onder de wettelijke uitzondering vallen, is geen toestemming nodig.

Voor tracking, advertentiecookies en andere niet-vrijgestelde toegang tot of opslag op je apparaat vragen wij vooraf toestemming. Deze technieken mogen pas worden geactiveerd nadat geldige toestemming is gegeven. Weigeren moet even eenvoudig zijn als accepteren. Je kunt een gegeven toestemming ook weer intrekken.

Waar een toestemmingsvenster wordt aangeboden, kun je daar je keuze maken en aanpassen. Je kunt cookies ook via je browser verwijderen of blokkeren. Daardoor werken bepaalde onderdelen, zoals inloggen of bestellen, mogelijk minder goed. Voor vragen over gebruikte technieken en bewaartermijnen kun je contact opnemen via support@hagehosting.com.

Ons contactformulier gebruikt hCaptcha van Intuition Machines, Inc. om geautomatiseerde inzendingen en misbruik te herkennen. Hierbij kunnen onder meer IP-adres, browser- en apparaatgegevens, tijdstippen en interacties met de controle worden verwerkt. Het doel is de beveiliging en beschikbaarheid van onze formulieren. Voor noodzakelijke beveiligingsverwerking beroepen wij ons op het gerechtvaardigd belang bij het voorkomen van misbruik, met een afweging van de gevolgen voor bezoekers. Waar toestemming vereist is voor toegang tot of opslag op je apparaat, moet die vooraf worden gegeven. Je kunt ons ook telefonisch of per e-mail bereiken.

Intuition Machines is gevestigd in de Verenigde Staten; verwerking buiten de EER kan plaatsvinden. De leverancier beschrijft standaardcontractbepalingen in zijn verwerkersaddendum voor de verwerking namens websitebeheerders. Zie voor aanvullende leveranciersinformatie https://www.hcaptcha.com/privacy. Je kunt ons vragen welke contractuele waarborgen op onze verwerking van toepassing zijn. Beveiligingsgegevens worden beperkt tot wat voor het vaststellen en

onderzoeken van misbruik nodig is; waar zij onderdeel zijn van onze eigen beveiligingslogs geldt de termijn van 180 dagen uit onderdeel 9.

11. Beveiliging van persoonsgegevens

Wij treffen passende technische en organisatorische maatregelen, rekening houdend met de risico's, de aard van de gegevens en de dienstverlening. Onze beveiligingsaanpak omvat, voor zover van toepassing op de dienst:

- beperking van toegang tot bevoegde personen en noodzakelijke rechten;
- passende authenticatie en aanvullende bescherming van beheeraccounts;
- beveiliging van gegevensoverdracht en bescherming van opgeslagen toegangsgegevens;
- onderhoud, updates en het beoordelen en verhelpen van kwetsbaarheden;
- bescherming tegen malware, spam en ongeoorloofde toegang;
- noodzakelijke logging, monitoring en onderzoek van beveiligingsincidenten;
- back-up- en herstelmaatregelen voor diensten waarvoor dit is overeengekomen;
- afspraken over vertrouwelijkheid en beveiliging met betrokken leveranciers.

Welke onderdelen Hage Hosting beheert en welke onderdelen jij beheert, hangt af van de overeenkomst. Bij een zelfbeheerde VPS kunnen bijvoorbeeld applicaties, gebruikersaccounts en updates binnen de server jouw verantwoordelijkheid zijn. Dit neemt onze eigen wettelijke verplichtingen niet weg.

De exacte beveiligingsinrichting verstrekken wij niet openbaar wanneer dat de beveiliging zou verzwakken. Relevante informatie voor klanten kan onder passende vertrouwelijkheidsafspraken beschikbaar worden gesteld. Beveiliging wordt beoordeeld en aangepast aan gewijzigde risico's; geen enkele beveiliging sluit ieder incident uit.

12. Datalekken, beveiligingsincidenten en Cyberbeveiligingswet

Vermoed je misbruik, een kwetsbaarheid of een datalek? Meld dit via support@hagehosting.com en bel bij spoed 0111-202088. Vermeld de betrokken dienst en wat je hebt waargenomen. Stuur niet meer persoonsgegevens of bewijsbestanden dan nodig en voer geen verdergaand onderzoek uit zonder toestemming.

Wij beoordelen incidenten en nemen noodzakelijke maatregelen om gevolgen te beperken en herstel mogelijk te maken. Wanneer een datalek onze eigen verwerking betreft, melden wij dit waar de AVG dat vereist zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur na kennisname aan de Autoriteit Persoonsgegevens. Bij een waarschijnlijk hoog risico informeren wij de betrokken personen onverwijld, behoudens wettelijke uitzonderingen.

Betreft een datalek persoonsgegevens die wij als verwerker voor een klant verwerken, dan informeren wij de verantwoordelijke klant zonder onredelijke vertraging en overeenkomstig de verwerkersovereenkomst. Wij wachten daarmee niet op het einde van een termijn die voor de melding door de klant aan een toezichthouder geldt. Wij ondersteunen de klant met beschikbare relevante informatie.

De Cyberbeveiligingswet is de Nederlandse uitwerking van de NIS2-richtlijn. Wanneer op onze dienstverlening verplichtingen uit deze wet of bijbehorende regels van toepassing zijn, kunnen wij persoonsgegevens verwerken voor beveiliging, wettelijk vereiste registratie, verificatie en incidentmelding. Deze meldingen hebben eigen criteria en termijnen en staan naast de

AVG-datalekmelding. Ook een incident zonder persoonsgegevens kan een meldingsplichtig beveiligingsincident zijn.

Voor incidentonderzoek en rechtmatige meldingen kunnen wij noodzakelijke contact-, technische en incidentgegevens delen met bevoegde autoriteiten en incidentresponsorganisaties. Wij beperken dit tot wat nodig en toegestaan is. Deze verklaring bevat geen aanspraak op certificering of een garantie dat een klant door het afnemen van onze diensten zelf aan NIS2 voldoet.

13. Geautomatiseerde beveiliging en besluitvorming

Beveiligingssystemen kunnen verdachte inlogpogingen, berichten, bestanden of verbindingen automatisch herkennen, tegenhouden of tijdelijk blokkeren. Dit dient de bescherming van de dienstverlening en wordt beperkt tot wat daarvoor nodig is. Denk je dat een blokkering onterecht is, neem dan contact op met onze support voor beoordeling.

Een automatisch beveiligingssignaal kan bijvoorbeeld leiden tot een tijdelijke beperking van een verbinding of bericht om misbruik te stoppen. Je kunt contact opnemen om de oorzaak en een mogelijke correctie te laten beoordelen. Voor uitsluitend geautomatiseerde besluiten met rechtsgevolgen of vergelijkbare aanmerkelijke gevolgen gelden aanvullende wettelijke voorwaarden en informatieplichten.

14. Gevoelige gegevens en minderjarigen

Wij vragen voor gewone dienstverlening niet standaard om een BSN, volledige kopie van een identiteitsbewijs of bijzondere persoonsgegevens. Voor sommige domeinregistraties en specifieke verificaties kunnen noodzakelijke identiteitsgegevens of een afgeschermde kopie nodig zijn, zoals toegelicht in onderdeel 6. Een aanvullende verificatie moet noodzakelijk en rechtmatig zijn. Een identiteitsdocument bevat gegevens met een verhoogd misbruikrisico; niet ieder gegeven daarop is juridisch een bijzonder persoonsgegeven in de zin van artikel 9 AVG. Als een verificatiemethode bijzondere persoonsgegevens verwerkt, moet daarvoor ook aan de aanvullende wettelijke voorwaarden zijn voldaan.

Gehoste klantdata kunnen wel gevoelige of bijzondere persoonsgegevens bevatten. De klant bepaalt welke gegevens rechtmatig mogen worden verwerkt en welke aanvullende afspraken en beveiliging nodig zijn. Waar wij zelf wettelijke verplichtingen hebben, blijven die gelden.

Onze dienstverlening richt zich niet specifiek op kinderen. Wanneer voor een rechtstreeks aangeboden online dienst aan een kind onder zestien jaar toestemming als grondslag wordt gebruikt, is in Nederland toestemming of machtiging van de ouder of wettelijke vertegenwoordiger nodig. Andere regels, bijvoorbeeld over het aangaan van overeenkomsten, kunnen daarnaast gelden. Neem contact op als je vermoedt dat wij onrechtmatig gegevens van een kind verwerken.

15. Jouw privacyrechten

Afhankelijk van de verwerking en de wettelijke voorwaarden heb je recht op inzage, correctie, verwijdering, beperking van de verwerking en overdraagbaarheid van gegevens. Je kunt bezwaar maken tegen verwerking op grond van een gerechtvaardigd belang. Bij direct marketing honoreren wij je bezwaar tegen het gebruik van je persoonsgegevens daarvoor.

Waar wij op basis van toestemming verwerken, kun je die toestemming intrekken. Dat verandert niet de rechtmatigheid van verwerking vóór de intrekking. Verwijdering is niet altijd mogelijk, bijvoorbeeld wanneer wij bepaalde gegevens wettelijk moeten bewaren.

Stuur je verzoek naar support@hagehosting.com, bij voorkeur vanuit je bekende e-mailadres of via je klantenaccount. Wij controleren je identiteit op een passende manier met zo min mogelijk aanvullende gegevens. Wij vragen niet standaard om een kopie van je identiteitsbewijs.

Wij reageren zonder onredelijke vertraging en in beginsel binnen één maand na ontvangst. Bij complexe of meerdere verzoeken kan de termijn wettelijk met maximaal twee maanden worden verlengd. Wij informeren je dan binnen de eerste maand over de verlenging en de reden. Een eventuele weigering lichten wij toe, met informatie over je klacht- en beroepsmogelijkheden.

Gaat je verzoek over gegevens die een klant bij ons host, dan is die klant doorgaans het juiste aanspreekpunt. Wij ondersteunen deze klant volgens onze verwerkersafspraken en wettelijke verplichtingen.

16. Klachten en wijzigingen

Heb je een vraag of klacht over onze verwerking? Neem contact op via support@hagehosting.com of bovenstaande contactgegevens. Je kunt ook rechtstreeks een klacht indienen bij de Autoriteit Persoonsgegevens: https://www.autoriteitpersoonsgegevens.nl. Je hoeft daarvoor niet eerst onze klachtenprocedure af te ronden.

Wij kunnen deze verklaring aanpassen bij wijzigingen in dienstverlening, verwerkingen of regelgeving. De actuele versie staat op onze website. Over belangrijke wijzigingen informeren wij je waar passend rechtstreeks. Een wijziging van deze verklaring vervangt geen toestemming wanneer daarvoor opnieuw toestemming nodig is.

Laatst bijgewerkt: 25 oktober 2026.