

Verwerkersovereenkomst

Dreamkit

VERSIE

2026-09-05 · geldende versie

VERWERKER

Bureau Bolster B.V., Rotterdam · KvK 61487953

CONTACT

Jaap Stronks · jaapstronks@bureaubolster.nl

Dit is de verwerkersovereenkomst die hoort bij elke Dreamkit-dienst. Door een Dreamkit-dienst af te nemen en de daarvoor verschuldigde vergoeding te voldoen, gaat u deze overeenkomst met Bureau Bolster B.V. (Dreamkit) aan; een aparte ondertekening is niet nodig (zie artikel 14). U kunt dit document hier downloaden en bewaren; de geldende versie staat ook op <https://dreamkit.eu/verwerkersovereenkomst>. Bij twijfel over de juridische strekking: laat een AVG-jurist meelezen. Dit is geen juridisch advies.

Inleiding — waar Dreamkit voor staat

Privacy, gegevensbescherming en digitale autonomie zijn voor Dreamkit geen sluitpost, maar **leidende ontwerpprincipes**. Wij bouwen websites en digitale infrastructuur voor maatschappelijke organisaties die het zich niet kunnen veroorloven dat de gegevens van hun achterban, donateurs of leden in handen vallen van partijen waarvan zij de governance niet kunnen beïnvloeden. Dat vertaalt zich in een aantal harde keuzes die deze verwerkersovereenkomst onderbouwt:

- 1. Geen afhankelijkheid van big tech voor de verwerking van persoonsgegevens.** De hosting, opslag, e-mailverzending, betaalverwerking en analytics waarop Dreamkit-klientsites draaien, zijn ondergebracht bij kleine, onafhankelijke Europese leveranciers — of bij door Dreamkit zelf beheerde servers. We kiezen bewust géén Google Cloud, Amazon Web Services, Microsoft Azure, Cloudflare, Mailchimp, Stripe, Vercel of vergelijkbare partijen, ook niet via hun Europese dochters.
- 2. Geen Amerikaanse diensten — ook geen Amerikaanse bedrijven met een Europese vestiging.** Onder de Amerikaanse *CLOUD Act* (Clarifying Lawful Overseas Use of Data Act, 2018) kunnen Amerikaanse autoriteiten gegevens vorderen die in beheer zijn van een Amerikaans bedrijf, ongeacht waar ter wereld die gegevens fysiek staan opgeslagen of welk dochterbedrijf er formeel eigenaar van is. Een Europese B.V., GmbH of S.A.S. die deel uitmaakt van een Amerikaans concern biedt daarom geen wezenlijke bescherming tegen extraterritoriale dataverzoeken. Wij vermijden dergelijke partijen waar mogelijk en zijn transparant over de schaarse uitzonderingen (zie bijlage A, sectie A.3).
- 3. Voorkeur voor zelf-gehoste, open-source software.** Analytics (Plausible), nieuwsbrievenverzending (Listmonk), serverbeheer (Ploi op eigen Hetzner-VPS'en), monitoring (Netdata) en spambescherming op formulieren (een zelf-gehoste proof-of-work-captcha in plaats van Google reCAPTCHA of Cloudflare Turnstile) draaien op infrastructuur die wij zelf beheren, met open broncode die door derden te auditen is. Daarmee worden gegevensstromen naar leveranciers geminimaliseerd: de leverancier levert de code, niet de toegang tot uw data.
- 4. Datasoevereiniteit op EU-bodem.** Persoonsgegevens worden uitsluitend opgeslagen en verwerkt binnen de Europese Economische Ruimte (EER), bij voorkeur in Duitsland, Nederland, Frankrijk of Finland. Er vindt geen structurele doorgifte plaats naar derde landen.

5. **Dataminimalisatie als uitgangspunt.** We bouwen formulieren, donatieflows en mailinglijsten die vragen wat nodig is, niet wat handig zou zijn voor latere analyse. Klanten worden waar relevant geadviseerd om bewaartermijnen te beperken en velden te schrappen.
6. **Transparantie over de keten.** Onze volledige lijst subverwerkers staat in bijlage A — geen verborgen partijen, geen onaangekondigde wijzigingen. Bij elke uitbreiding of vervanging van een subverwerker krijgt u vooraf bericht en de gelegenheid om bezwaar te maken (zie artikel 7).

Deze principes maken Dreamkit niet de goedkoopste of de meest schaalbare leverancier. Ze maken Dreamkit wel een leverancier waarbij u uw achterban met droge ogen kunt vertellen dat hun gegevens niet doorverkocht, geprofileerd of door buitenlandse overheden opvraagbaar zijn.

Partijen

Verwerkingsverantwoordelijke (hierna: "Klant")

- De organisatie die een Dreamkit-dienst afneemt. De gegevens van Klant (naam, rechtsvorm, KvK-/ondernemingsnummer, adres en contactpersoon voor AVG-aangelegenheden) zijn vastgelegd in de Hoofdovereenkomst en in de bij Dreamkit geregistreerde accountgegevens van Klant.

Verwerker (hierna: "Dreamkit" of "Verwerker")

- Bureau Bolster B.V., handelend onder de naam Dreamkit
- Gevestigd te Rotterdam
- KvK: 61487953
- Vertegenwoordigd door: Jaap Stronks
- Contact voor AVG-aangelegenheden: jaapstronks@bureaubolster.nl

Hierna gezamenlijk te noemen: "Partijen".

Overwegingen

- Klant en Dreamkit hebben een dienstverleningsovereenkomst gesloten op grond waarvan Dreamkit voor Klant een website, hostingomgeving en/of gerelateerde digitale diensten levert (de "Hoofdovereenkomst").
- Bij het leveren van deze diensten verwerkt Dreamkit persoonsgegevens namens Klant.
- Op grond van artikel 28 van de Algemene Verordening Gegevensbescherming (AVG) zijn Partijen verplicht de verwerking schriftelijk vast te leggen.
- Deze verwerkersovereenkomst (hierna: "Verwerkersovereenkomst") maakt onlosmakelijk deel uit van de Hoofdovereenkomst.

1. Definities

Term	Betekenis
AVG	Verordening (EU) 2016/679 (Algemene Verordening Gegevensbescherming).
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals bedoeld in artikel 4 lid 1 AVG.

Term	Betekenis
Verwerking	Elke bewerking van Persoonsgegevens zoals bedoeld in artikel 4 lid 2 AVG.
Betrokkene	De natuurlijke persoon op wie de Persoonsgegevens betrekking hebben.
Subverwerker	Derde partij die door Dreamkit wordt ingeschakeld bij de Verwerking.
Datalek	Inbreuk in verband met Persoonsgegevens, zoals bedoeld in artikel 4 lid 12 AVG.
EER	Europese Economische Ruimte.

2. Onderwerp en duur

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Dreamkit in het kader van de Hoofdovereenkomst.

2.2 De Verwerkersovereenkomst geldt voor de duur van de Hoofdovereenkomst en blijft van kracht zolang Dreamkit Persoonsgegevens van Klant onder zich houdt.

2.3 Beëindiging van de Hoofdovereenkomst beëindigt automatisch deze Verwerkersovereenkomst, onverminderd artikel 11 (teruggave en vernietiging).

3. Aard, doel en categorieën

3.1 **Aard van de Verwerking.** Hosting van de website van Klant; opslag en doorgifte van formulier-inzendingen; verzending van transactionele e-mail en — indien overeengekomen — nieuwsbrieven; verwerking van donaties of betalingen; geanonimiseerde bezoekersstatistieken; backups; technisch beheer en onderhoud.

3.2 **Doel van de Verwerking.** Het mogelijk maken dat Klant haar achterban, leden, donateurs en bezoekers kan bereiken, registreren en bedienen via de door Dreamkit geleverde digitale infrastructuur.

3.3 **Categorieën Betrokkenen.** Bezoekers van de website van Klant; afzenders van contact- of aanmeldformulieren; nieuwsbriefabonnees; donateurs of betalers; leden en/of vrijwilligers; redacteurs en beheerders aan zijde van Klant.

3.4 **Categorieën Persoonsgegevens.** Afhankelijk van de specifieke configuratie kan het gaan om: naam, e-mailadres, telefoonnummer, adresgegevens, IP-adres (kortstondig, voor beveiliging, fraude- en spampreventie), donatiebedrag en -frequentie, betaalkenmerken (geen volledige IBAN of kaartnummer — die blijven bij de betaaldienstverlener), inhoud van berichten en formulier-inzendingen, accountcredentials van redacteurs (gehasht), en eventuele aanvullende velden die Klant zelf in formulieren of CRM-velden definieert.

3.5 **Bijzondere categorieën Persoonsgegevens** (artikel 9 AVG) worden in beginsel **niet** door Dreamkit verwerkt. Indien Klant voornemens is bijzondere categorieën te verwerken (bijv. politieke voorkeur via een ledenadministratie, of gezondheidsgegevens via een meldpunt), is **voorafgaande schriftelijke afstemming** vereist over passende aanvullende waarborgen.

3.6 **Deelverwerking: supporterregistratie.** Dreamkit voegt de gegevens die via de afzonderlijke Dreamkit-onderdelen (formulier-inzendingen, donaties, nieuwsbrief-inschrijvingen, supportcontacten) al namens Klant worden verwerkt, samen tot één geünificeerd supporterbeeld per Klant. Het doel is **administratieve ontlasting en ondersteuning**: Klant kan haar achterban in samenhang inzien, rapportages opstellen en

verzoeken van Betrokkenen (inzage, export, verwijdering) in één handeling afhandelen in plaats van verspreid over losse systemen. Deze deelverwerking introduceert **geen nieuwe gegevensverzameling**: alle gegevens stonden al op Dreamkit-beheerde systemen onder deze Verwerkersovereenkomst. De supporterregistratie is een wijziging in de *middelen* van bestaande verwerkingen, aangevuld met dit met de oorspronkelijke doeleinden verenigbare doel (administratie en support). Verdere doeleinden zoals gedragssegmentatie of gerichte campagnevoering vallen hier niet onder en vergen een afzonderlijke, expliciete keuze van Klant.

3.6.1 Twee standen. (a) *Geaggregeerde rapportage* — anonieme tellers per campagne, event-type en periode, zonder identifiers. Deze stand verwerkt geen Persoonsgegevens en staat voor elke Klant aan. (b) *Supporterbeeld* — opslag van Persoonsgegevens per supporter (zie 3.6.2) met tijdlijn, zoekfunctie en AVG-export/-verwijdering. Deze stand wordt geactiveerd ná de notificatie en bezwaartermijn van artikel 7A. Maakt Klant bezwaar (zie 7A.3), dan draait de betreffende omgeving uitsluitend in de geaggregeerde, anonieme stand en worden er geen Persoonsgegevens in een supporterbeeld opgeslagen.

3.6.2 Categorieën Persoonsgegevens in het supporterbeeld. Naam en e-mailadres; donatiegeschiedenis (bedrag, frequentie, status; geen volledige IBAN of kaartnummer); ondertekeningen van petitie en formulieren; nieuwsbrief-inschrijvingen en de toestemmingsstatus per onderwerp (inclusief herkomst en tijdstip); en verwijzingen naar supportcontacten. Er worden geen nieuwe velden verzameld buiten wat Klant al via haar formulieren, donatieflows, nieuwsbrief en support vergaart.

3.6.3 Bewaartermijnen. Geaggregeerde, anonieme tellers worden onbeperkt bewaard; zij bevatten geen Persoonsgegevens. Persoonsgegevens in het supporterbeeld worden bewaard zolang de onderliggende bronregistratie bestaat en de relatie tussen Betrokkene en Klant voortduurt. Bij verwijdering van de bronregistratie, een verwijderingsverzoek van de Betrokkene, of beëindiging van de Hoofdovereenkomst worden zij verwijderd conform artikel 11. Een ingetrokken toestemming (bijvoorbeeld een nieuwsbrief-afmelding) wordt verwerkt als statuswijziging; uitsluitend een geminimaliseerd suppressie-kenmerk (zoals een gehasht e-mailadres) kan daarna worden bewaard, met als enige doel te voorkomen dat een afgemelde Betrokkene opnieuw wordt aangeschreven.

3.6.4 Bijzondere categorieën in het supporterbeeld. Voor zover het supporterbeeld bij politiek of levensbeschouwelijk geprofileerde Klanten gegevens bevat die als bijzondere categorie (artikel 9 AVG) kunnen kwalificeren — zoals het ondertekenen van een politieke petitie of een lidmaatschap — verandert de risicoklasse niet ten opzichte van de bestaande losse verwerking van diezelfde gegevens. Onverkort gelden de waarborgen van bijlage B, in het bijzonder encryptie althans, verwerking uitsluitend binnen de EER, en strikte scheiding tussen Klanten (supporters worden nooit over Klanten heen gekoppeld).

4. Verplichtingen van Dreamkit

4.1 Dreamkit verwerkt Persoonsgegevens uitsluitend op basis van schriftelijke (waaronder elektronische) instructies van Klant, behoudens afwijkende wettelijke verplichtingen.

4.2 Dreamkit waarborgt dat personen die onder haar gezag werken en toegang hebben tot Persoonsgegevens, deze uitsluitend verwerken in opdracht van Klant en gebonden zijn aan vertrouwelijkheid.

4.3 Dreamkit neemt de in bijlage B beschreven passende technische en organisatorische maatregelen, zoals bedoeld in artikel 32 AVG.

4.4 Dreamkit ondersteunt Klant — voor zover redelijkerwijs mogelijk — bij het voldoen aan haar verplichtingen op grond van de artikelen 32 t/m 36 AVG (beveiliging, meldplicht, DPIA, voorafgaande raadpleging).

4.5 Dreamkit verwerkt geen Persoonsgegevens buiten de EER, tenzij dat noodzakelijk is voor de overeengekomen dienst én tussen Partijen schriftelijk is afgesteld en passende waarborgen (zoals de modelcontractbepalingen van de Europese Commissie) zijn ingeregeld. De huidige stand van zaken: er vindt **geen** structurele doorgifte buiten de EER plaats. Zie bijlage A.3 voor de incidentele uitzonderingen (uitsluitend technische metadata; geen Persoonsgegevens van Betrokkenen).

5. Verplichtingen van Klant

5.1 Klant is en blijft verwerkingsverantwoordelijke in de zin van de AVG en is verantwoordelijk voor de rechtmatigheid van de Verwerking, inclusief de grondslag, het informeren van Betrokkenen en het verkrijgen van toestemming waar vereist.

5.2 Klant zorgt ervoor dat haar instructies aan Dreamkit niet in strijd zijn met de AVG of andere toepasselijke wetgeving.

5.3 Klant draagt zorg voor een actuele privacyverklaring op haar website, waarin de hier beschreven Verwerking en subverwerkers worden vermeld of in elk geval samengevat. Dreamkit levert hiervoor desgevraagd standaardtekstvoorstellen aan.

6. Beveiliging

6.1 Dreamkit treft passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies, ongeoorloofde toegang, vernietiging of wijziging. De huidige maatregelen zijn beschreven in bijlage B.

6.2 De maatregelen worden periodiek geëvalueerd en — waar nodig — aangescherpt aan de stand van de techniek, de aard van de gegevens en het risico voor Betrokkenen.

7. Subverwerkers

7.1 Dreamkit schakelt voor de uitvoering van de Hoofdovereenkomst subverwerkers in. De actuele lijst staat in **bijlage A**.

7.2 Klant geeft hierbij **algemene voorafgaande toestemming** voor het inschakelen van de in bijlage A genoemde subverwerkers.

7.3 Dreamkit informeert Klant ten minste **dertig (30) dagen** voor de invoering van een nieuwe subverwerker of vervanging van een bestaande, schriftelijk (per e-mail volstaat). Klant heeft binnen die termijn het recht gemotiveerd bezwaar te maken op grond van AVG-redenen. Bij gegrond bezwaar zoeken Partijen in onderling overleg naar een alternatief; lukt dat niet, dan heeft Klant het recht de Hoofdovereenkomst te beëindigen zonder dat dit een tekortkoming oplevert.

7.4 Dreamkit legt subverwerkers schriftelijk dezelfde of vergelijkbare verplichtingen op als die voor Dreamkit voortvloeien uit deze Verwerkersovereenkomst.

7.5 Dreamkit blijft tegenover Klant volledig aansprakelijk voor de naleving van deze Verwerkersovereenkomst door subverwerkers.

7A. Wijzigingen in de verwerking en nieuwe deelverwerkingen

7A.1 Dreamkit kan de middelen of doeleinden van de Verwerking aanpassen of een nieuwe deelverwerking toevoegen, mits deze verenigbaar is met de oorspronkelijke doeleinden en binnen de kaders van deze Verwerkersovereenkomst blijft. Voor verwerkingen met een wezenlijk nieuw doel dat niet verenigbaar is met de oorspronkelijke doeleinden, is een afzonderlijke, expliciete keuze of toestemming van Klant vereist.

7A.2 Dreamkit informeert Klant ten minste **dertig (30) dagen** vóór de invoering van een nieuwe deelverwerking die Persoonsgegevens betreft, schriftelijk (per e-mail volstaat), onder vermelding van het doel, de betrokken categorieën Persoonsgegevens en de bewaartermijnen.

7A.3 Klant heeft binnen die termijn het recht gemotiveerd bezwaar te maken op grond van AVG-redenen. Bij bezwaar tegen de supporterregistratie (artikel 3.6) draait de betreffende omgeving uitsluitend in de geaggregeerde, anonieme stand (artikel 3.6.1 onder a); er worden dan geen Persoonsgegevens in een supporterbeeld opgeslagen, en aanwezige supporterbeeld-gegevens worden niet aangemaakt of verwijderd. Voor andere deelverwerkingen zoeken Partijen bij gegrond bezwaar in onderling overleg naar een passende oplossing; artikel 7.3, laatste zin (beëindigingsrecht zonder dat dit een tekortkoming oplevert), is van overeenkomstige toepassing.

7A.4 Het uitblijven van bezwaar binnen de termijn geldt als aanvaarding van de gewijzigde of nieuwe deelverwerking. Klant kan ook ná de termijn alsnog bezwaar maken; vanaf dat moment schakelt Dreamkit de betreffende omgeving om naar de geaggregeerde, anonieme stand. Nieuwe Klanten aanvaarden de op het moment van aangaan geldende versie van deze Verwerkersovereenkomst (artikel 14).

8. Rechten van Betrokkenen

8.1 Indien een Betrokkene een verzoek doet tot inzage, rectificatie, verwijdering, beperking, dataportabiliteit of bezwaar (artikelen 15 t/m 22 AVG), en dit verzoek bij Dreamkit binnenkomt, stuurt Dreamkit het verzoek onverwijld door naar Klant en behandelt het niet zelf.

8.2 Dreamkit assisteert Klant — voor zover redelijkerwijs mogelijk en tegen redelijke kosten — bij het beantwoorden van dergelijke verzoeken. Voor standaardacties (export, anonimisering, verwijdering uit nieuwsbrief-database) worden geen kosten in rekening gebracht; voor maatwerk-extracties kan een uurtarief gelden conform de Hoofdovereenkomst.

9. Datalekken

9.1 Dreamkit meldt elk Datalek **zonder onredelijke vertraging en uiterlijk binnen 24 uur** na ontdekking aan Klant, schriftelijk (per e-mail aan het in artikel "Partijen" genoemde contactadres).

9.2 De melding bevat in elk geval:

- de aard van het Datalek;
- de (geschatte) omvang: aantal Betrokkenen, aantal records, betrokken categorieën gegevens;
- de waarschijnlijke gevolgen;

- de getroffen en nog te treffen maatregelen.

9.3 Klant is verantwoordelijk voor de eventuele melding aan de Autoriteit Persoonsgegevens (artikel 33 AVG) en aan Betrokkenen (artikel 34 AVG). Dreamkit ondersteunt deze meldingen inhoudelijk.

9.4 Dreamkit houdt een intern register bij van Datalekken — ongeacht of melding aan de toezichthouder geboden is — en deelt dit op verzoek met Klant.

10. Audit

10.1 Klant heeft het recht om — maximaal éénmaal per jaar, en in geval van een gemeld Datalek — door middel van een schriftelijke vragenlijst of een audit door een onafhankelijke derde te (laten) controleren of Dreamkit aan deze Verwerkersovereenkomst voldoet.

10.2 Audits worden ten minste **vier (4) weken** van tevoren aangekondigd en zo uitgevoerd dat de bedrijfsvoering van Dreamkit en haar andere klanten zo min mogelijk wordt verstoord.

10.3 Kosten van een audit komen voor rekening van Klant, tenzij uit de audit een wezenlijke tekortkoming aan zijde van Dreamkit blijkt — in dat geval draagt Dreamkit de redelijke kosten.

11. Teruggave en vernietiging

11.1 Bij beëindiging van de Hoofdovereenkomst, of op eerder verzoek van Klant, draagt Dreamkit Persoonsgegevens binnen **dertig (30) dagen** over aan Klant (in een gangbaar machineleesbaar formaat zoals SQL-dump, CSV of JSON) of vernietigt Dreamkit ze onomkeerbaar — naar keuze van Klant.

11.2 Backups die niet onmiddellijk verwijderbaar zijn (vanwege rolling-backup-vensters), worden uiterlijk **90 dagen** na beëindiging vernietigd. Tijdens die overgangsperiode blijven de waarborgen van deze Verwerkersovereenkomst van kracht.

11.3 Dreamkit bevestigt vernietiging op verzoek schriftelijk.

12. Aansprakelijkheid

12.1 De aansprakelijkheid van Dreamkit uit hoofde van deze Verwerkersovereenkomst is onderworpen aan de aansprakelijkheidsregeling van de Hoofdovereenkomst, met dien verstande dat een eventuele beperking van aansprakelijkheid niet geldt voor opzet of bewuste roekeloosheid en evenmin voor boetes die direct aan Klant worden opgelegd door de Autoriteit Persoonsgegevens als gevolg van een toerekenbare tekortkoming van Dreamkit.

13. Slotbepalingen

13.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

13.2 Geschillen worden voorgelegd aan de bevoegde rechter in het arrondissement Rotterdam.

13.3 Indien een bepaling uit deze Verwerkersovereenkomst nietig of vernietigbaar blijkt, blijven de overige bepalingen van kracht en vervangen Partijen de getroffen bepaling in overleg door een geldige bepaling die het oorspronkelijke doel zoveel mogelijk benadert.

13.4 Wijzigingen op deze Verwerkersovereenkomst zijn slechts geldig indien schriftelijk (waaronder elektronisch) overeengekomen tussen Partijen. Dreamkit kan de subverwerkerslijst (bijlage A) actualiseren volgens de procedure van artikel 7.3.

13.5 Bij strijdigheid tussen de Hoofdovereenkomst en deze Verwerkersovereenkomst, prevaleert deze Verwerkersovereenkomst voor zover het de Verwerking van Persoonsgegevens betreft.

13.6 De Nederlandse tekst van deze Verwerkersovereenkomst is de authentieke tekst. Dreamkit kan vertalingen beschikbaar stellen ter informatie; bij verschil tussen een vertaling en de Nederlandse tekst prevaleert de Nederlandse tekst.

14. Totstandkoming en aanvaarding

14.1 Deze Verwerkersovereenkomst maakt onlosmakelijk deel uit van de Hoofdovereenkomst (zie de Overwegingen en artikel 13.5).

14.2 Door het aangaan van de Hoofdovereenkomst — het afnemen van een Dreamkit-dienst en het voldoen van de daarvoor verschuldigde vergoeding — aanvaardt Klant deze Verwerkersovereenkomst. Een afzonderlijke ondertekening is niet vereist: aanvaarding langs elektronische weg voldoet aan het schriftelijkheidsvereiste van artikel 28 lid 9 AVG.

14.3 De geldende versie van deze Verwerkersovereenkomst is doorlopend openbaar beschikbaar op <https://dreamkit.eu/verwerkersovereenkomst> en voor Klant te downloaden en te bewaren via de Dreamkit-klantomgeving. Dreamkit bewaart de eerdere versies en stelt op verzoek van Klant vast welke versie op een bepaald moment gold.

14.4 Deze Verwerkersovereenkomst geldt platform-breed en is voor elke Klant gelijk. Wat een Klant feitelijk afneemt, en daarmee welke van de in bijlage A genoemde subverwerkers voor die Klant worden ingeschakeld, volgt uit de Hoofdovereenkomst en de in de Dreamkit-klantomgeving geregistreerde diensten. Afwijkende of aanvullende verwerkingen die uitsluitend voor één Klant gelden, worden vastgelegd in een addendum dat naar deze Verwerkersovereenkomst en de versie daarvan verwijst.

Bijlage A — Subverwerkers

Stand: **2026-06-15**. Deze bijlage wordt geactualiseerd wanneer Dreamkit een subverwerker toevoegt, vervangt of beëindigt; wijzigingen worden conform artikel 7.3 aangekondigd.

Niet elke in deze bijlage genoemde partij is voor elke Klant van toepassing. Wat er feitelijk wordt ingeschakeld, hangt af van de door Klant geactiveerde functies. De nieuwsbrief functie zet Listmonk in (zelf-gehost; zie A.2); de betaal functie zet de Pronamic-plugin in (zelf-gehost; zie A.2), gekoppeld aan het eigen betaalaccount van Klant (zie de noot onder A.2); hosting bij Raidboxes geldt alleen voor sites die nog niet naar de Hetzner/Ploi-omgeving zijn gemigreerd. De vaste infrastructuur (hosting, backups, transactionele e-mail, DNS, analytics, monitoring) geldt voor elke Klant.

A.1 Hoofdsbverwerkers — verwerken namens Klant Persoonsgegevens

Subverwerker	Land / regio	Functie	Categorieën gegevens	Waarborgen
Hetzner Online GmbH	Duitsland (Falkenstein/ Nürnberg)	VPS-hosting voor Dreamkit-platform: WordPress-installaties, database (MariaDB), Plausible-analytics, Listmonk-nieuwsbrieven, supporter-registry, Netdata-monitoring	Alle in artikel 3.4 genoemde categorieën	EU-leverancier; AVG-conforme verwerkersovereenkomst; ISO 27001
Hetzner Storage Box	Finland (Helsinki)	Off-site versleutelde backups (restic-encrypted)	Volledige backups van klantsites	Encryptie at rest met door Dreamkit beheerde sleutel; toegang uitsluitend vanaf Dreamkit-IP
Ploi B.V.	Nederland	Server-control-panel: provisioning, deploys, monitoring-dashboard voor Hetzner-VPS'en	Beperkt — Ploi heeft administratieve toegang tot servers maar verwerkt zelf geen klantdata structureel	Nederlandse leverancier; verwerkersovereenkomst beschikbaar
Raidboxes GmbH	Duitsland (Bremen)	Managed WordPress-hosting (legacy-omgeving — wordt gefaseerd uitgefaseerd ten gunste van Hetzner/Ploi)	Alle in artikel 3.4 genoemde categorieën, voor sites die nog niet gemigreerd zijn	Duitse leverancier; AVG-conforme verwerkersovereenkomst
Scaleway SAS	Frankrijk (Paris)	(a) Transactional Email (TEM) — verzending van transactionele e-mails (b) Object Storage — secundaire off-site backups	(a) E-mailadressen ontvangers + berichtinhoud (b) Volledige backups	Franse leverancier; SOC 2 + ISO 27001; Object Lock + versioning aan

A.2 Zelf-gehoste software en ondersteunende diensten — geen subverwerkers in de zin van artikel 28 AVG

De onderstaande componenten zijn **geen subverwerkers in de zin van artikel 28 AVG**. Het gaat om door Dreamkit zelf-gehoste open-source software (draait op onze eigen infrastructuur; er gaat geen data naar een derde partij) of om diensten die uitsluitend technische metadata verwerken. We noemen ze hier voor volledige transparantie.

Component	Land	Functie	Waarom geen subverwerker
deSEC e.V.	Duitsland (Berlijn)	DNS-hosting voor dreamkit.eu en klant domeinen	Verwerkt geen Persoonsgegevens van Betrokkenen; alleen DNS-records (technische metadata)
HetrixTools SRL	Roemenië	Externe uptime-monitoring (HTTP-probes)	Probet uitsluitend openbare URLs; geen toegang tot databases of inhoud

Component	Land	Functie	Waarom geen subverwerker
Plausible (self-hosted)	Eigen Hetzner-VPS, Duitsland	Cookieless web-analytics	Verwerkt geanonimiseerde paginabezoeken; geen IP-opslag, geen cookies, geen profilering. Plausible Insights OÜ (Estland) levert de broncode maar heeft geen toegang tot de data
Listmonk (self-hosted)	Eigen Hetzner-VPS, Duitsland	Nieuwsbrievenverzending — <i>alleen als Klant de nieuwsbrieffunctie gebruikt</i>	Open-source mailinglijst-software die op Dreamkit-infrastructuur draait; data blijft op die infrastructuur, er gaat niets naar een derde partij
Pronamic Pay (self-hosted)	Nederland (lokaal op de hosting)	Betaal-plugin: koppelt de site aan een betaaldienst — <i>alleen als Klant de betaalfunctie gebruikt</i>	Open-source WordPress-plugin die lokaal op de Dreamkit-hosting draait; stuurt zelf geen data naar Pronamic. Betalingen lopen naar het eigen betaalaccount van Klant (zie noot)
Netdata (self-hosted)	Eigen Hetzner-VPS, Duitsland	Server-performance-monitoring (CPU/RAM/disk)	Geen Persoonsgegevens van Betrokkenen; alleen serverstatistieken. Geen Netdata Cloud-koppeling
Supporter-registry (self-hosted)	Eigen Hetzner-VPS, Duitsland	Geünificeerd supporterbeeld per Klant: voegt bestaande formulier-, donatie-, nieuwsbrief- en supportgegevens samen tot één beeld t.b.v. administratie en support (zie artikel 3.6)	Door Dreamkit zelf ontwikkelde software die op Dreamkit-infrastructuur draait; data blijft op die infrastructuur en gaat niet naar een derde partij. Geen aparte subverwerker — Dreamkit is en blijft Verwerker voor deze deelverwerking
Wings-ALTCHA anti-spam (self-hosted)	Eigen Hetzner-VPS, Duitsland	Proof-of-work-captcha tegen bot- en spam-inzendingen op formulieren — <i>alleen op formulieren waarvoor Klant het inschakelt</i>	Door Dreamkit zelf ontwikkelde plugin bovenop de open-source ALTCHA-core (MIT); widget en challenge-verificatie draaien volledig op Dreamkit-infrastructuur, zonder externe call of CDN. Vervangt bewust Google reCAPTCHA / Cloudflare Turnstile (VS). Verwerkt het IP-adres uitsluitend kortstondig voor rate-limiting; geen profilering, geen doorgifte aan derden

Betalingen en het eigen betaalaccount van Klant. Donaties en betalingen op de site verlopen via de Pronamic-plugin naar het account dat **Klant zelf** bij een betaaldienstverlener (zoals Mollie) aanhoudt. Die betaaldienstverlener verwerkt de betaalgegevens als verwerker van **Klant**, niet van Dreamkit; Dreamkit heeft geen toegang tot dat account. Dit is vergelijkbaar met situaties waarin Klant zelf een externe dienst (zoals Mailchimp) op de site koppelt: die relatie valt buiten deze Verwerkersovereenkomst en is een eigen verantwoordelijkheid van Klant.

A.3 Componenten van Amerikaanse herkomst — strikt beperkt en transparant gemaakt

Wij voeren een actief beleid om Amerikaanse diensten te vermijden, inclusief Amerikaanse moederconcerns met Europese dochters (zie inleiding, principe 2). Op dit moment resteren de volgende **technisch onvermijdelijke** of **uitgefaseerde** Amerikaanse aanrakingen. Geen van deze componenten verwerkt Persoonsgegevens van Betrokkenen van Klant:

Component	Amerikaanse partij	Wat het doet	Waarom (nog) niet vermeden	Welke gegevens raakt het
Gravity Forms	Rocketgenius Inc. (VS)	WordPress-formulierenplugin	Marktleidende plugin voor complexe formulieren; geen volwaardig EU-alternatief met dezelfde functionaliteit. We onderzoeken vervanging.	Geen Persoonsgegevens van Betrokkenen. Alleen periodieke licentie-validatie (license key + domeinnaam) — formulier-inzendingen blijven volledig in de WordPress-database op Hetzner.
GitHub (Microsoft)	GitHub Inc. (VS, onderdeel van Microsoft)	Versiebeheer van de Dreamkit-broncode	Vrijwel de gehele open-source-wereld leeft op GitHub; migratie naar Codeberg / self-hosted Forgejo is op de roadmap.	Geen Persoonsgegevens van Betrokkenen. Bevat uitsluitend code, geen klantdata, geen formulier-inzendingen, geen ledenlijsten.

Beleid Notion: Bureau Bolster gebruikt Notion intern voor projectplanning, maar laat hier **uitdrukkelijk geen gegevens van Klant-websites of haar Betrokkenen doorheen lopen**. Klantcontactgegevens en projectaantekeningen die in Notion belanden, beperken zich tot de directe contactpersonen bij Klant zelf (naam, e-mail, gespreksverslagen) — geen achterban-, donateur-, leden- of bezoekersgegevens.

Als Klant bezwaar heeft tegen één of meer van de bovenstaande componenten, kan Dreamkit in overleg een afwijkende configuratie inrichten (bijv. Gravity Forms vervangen door een open-source-alternatief). De praktische gevolgen worden dan vooraf besproken.

Bijlage B — Technische en organisatorische maatregelen

De volgende maatregelen geven invulling aan artikel 32 AVG. Ze worden ten minste jaarlijks geëvalueerd.

B.1 Toegangsbeveiliging

- SSH-toegang tot servers uitsluitend via Ed25519-publieke sleutels in 1Password-vault. Geen wachtwoord-authenticatie op SSH.
- Tweefactor-authenticatie verplicht voor alle beheerinterfaces (Ploi, Hetzner Cloud Console, Scaleway-console, Mollie-dashboard, Raidboxes-dashboard, GitHub).
- Beheerinterface-toegang tot servers via Ploi is per beheerder geoormerkt en logbaar.
- WordPress-beheeraccounts gebruiken sterke wachtwoorden + tweefactor (waar de plugin-stack dat ondersteunt).

B.2 Encryptie

- TLS 1.2+ verplicht op alle openbare endpoints (Let's Encrypt of vergelijkbare CA).
- Backups versleuteld at rest met `restic` (AES-256), met sleutels beheerd in 1Password.
- Wachtwoorden in WordPress opgeslagen als bcrypt-hash (WordPress-default).

B.3 Segmentatie, isolatie en scheiding van klantgegevens

- **Scheiding van klantgegevens:** elke klantsite draait op een eigen WordPress-installatie met een eigen database; Persoonsgegevens van een Klant worden uitsluitend verwerkt voor de dienstverlening aan die Klant en zijn gescheiden van de gegevens van andere klanten.
- Hetzner Cloud Firewall (`dreamkit-web`): inbound uitsluitend TCP 22/80/443 + ICMP; uitgaand vrij.
- Netdata, Plausible en MariaDB gebonden aan `127.0.0.1` of het private Hetzner-netwerk; geen openbare blootstelling.
- Backup-Storage Box (Hetzner Helsinki): External Reachability staat **uit**; alleen bereikbaar vanaf Dreamkit-IP's via key-auth.

B.4 Backups en herstelbaarheid

- **3-2-1-strategie:** dagelijkse `restic`-backups, twee off-site kopieën (Hetzner Storage Box in Helsinki + Scaleway Object Storage in Paris), één primaire kopie op de app-box.
- Backup-versleuteling met door Dreamkit beheerde sleutel.
- Periodieke restore-drills (≥ jaarlijks); resultaat gelogd in `docs/hosting/restore-drill.md`.
- RTO/RPO: doel-RTO ≤ 4 uur, doel-RPO ≤ 24 uur (Fase 1).

B.5 Logging en monitoring

- Netdata op alle app-boxen voor CPU/RAM/disk/MariaDB-alerts.
- HetrixTools voor externe uptime-monitoring (1-minuut-check vanuit EU-locaties).

- WordPress security-plugin logt loginpogingen en blokkeert bij brute force.

B.6 Personele waarborgen

- Op dit moment is Bolster een éénpersoonsbedrijf; alleen Jaap Stronks heeft toegang tot productiesystemen.
- Bij uitbreiding van het team worden vertrouwelijkheidsverklaringen ondertekend voor toegang tot Persoonsgegevens.
- Geen onderaannemers met directe toegang tot Persoonsgegevens zonder voorafgaande schriftelijke instemming van Klant.

B.7 Software-onderhoud

- WordPress core + plugins worden ten minste maandelijks bijgewerkt.
- Kritieke beveiligingsupdates worden binnen 7 dagen na publicatie uitgerold.
- Onderhoudsstatus per klantsite traceerbaar in [docs/hosting/](#).

B.8 Datalek-respons

- Bij vermoeden van een Datalek wordt een interne checklist gevolgd: containment → impact-analyse → klant-notificatie binnen 24 uur → herstelmaatregelen → evaluatie.
- Datalek-register wordt bijgehouden, ook voor incidenten die niet aan de AP gemeld hoefden te worden.

Einde verwerkersovereenkomst.