**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

# VERWERKERSOVEREENKOMST (DATA PROCESSING AGREEMENT)

**Versie:** 1.9.1 **Datum:** 21 oktober 2026 **Gebaseerd op:** Artikel 28 AVG (Verordening (EU) 2016/679) en UAVG **Publicatielocatie:** `https://noveu.eu/juridisch/verwerkersovereenkomst`

> *Deze Verwerkersovereenkomst ("DPA") maakt onlosmakelijk deel uit van de Overeenkomst tussen Opdrachtgever (Verwerkingsverantwoordelijke) en Noveu Solutions (Verwerker) en prevaleert op de Algemene Voorwaarden voor zover het de verwerking van Persoonsgegevens betreft.*

---

## PARTIJEN

**1. Verwerkingsverantwoordelijke ("Opdrachtgever"):**

| | |
|---|---|
| Bedrijfsnaam | `[Bedrijfsnaam klant]` |
| Vestigingsadres | `[Adres], [Postcode] [Plaats]` |
| KvK-nummer | `[KvK-nummer]` |
| Vertegenwoordigd door | `[Naam], [Functie]` |
| Contact (privacy) | `[E-mailadres]` |

**2. Verwerker:**

| | |
|---|---|
| Bedrijfsnaam | Noveu Solutions |
| Vestigingsadres | Graskarpersingel 52, 2492 MV 's-Gravenhage |
| KvK-nummer | 42030979 |
| Vertegenwoordigd door | M. de Visser, eigenaar |
| Contact (privacy) | `privacy@noveu.eu` |

Hierna gezamenlijk: **Partijen**.

---

## OVERWEGINGEN

A. Partijen hebben een hoofdovereenkomst gesloten op grond waarvan Noveu Diensten levert, waaronder mogelijk: Noveu Workspace (SaaS), Noveu Webmail/Mail Hosting, Noveu Hosting, NoveuFlow (een WordPress-plugin die op de website van Opdrachtgever draait), Managed IT, API- en AI-diensten (hierna: de **"Hoofdovereenkomst"**).

B. Bij de uitvoering van de Hoofdovereenkomst verwerkt Noveu Persoonsgegevens ten behoeve van Opdrachtgever in de zin van de AVG.

C. Deze DPA voldoet aan artikel 28 lid 3 AVG en de UAVG en is gebaseerd op de NLdigital-modelverwerkersovereenkomst, aangepast aan de specifieke dienstverlening van Noveu.

---

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

## ARTIKEL 1: DEFINITIES

1.1. Termen met een hoofdletter die in deze DPA niet anders zijn gedefinieerd, hebben de betekenis uit de AVG of de Algemene Voorwaarden van Noveu.

1.2. **Datalek:** een inbreuk op de beveiliging die per ongeluk of onrechtmatig leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of toegang tot Persoonsgegevens.

1.3. **Sub-verwerker:** een derde die door Noveu wordt ingeschakeld om (een deel van) de Persoonsgegevens te verwerken.

1.4. **Toezichthouder:** de Autoriteit Persoonsgegevens (AP) of een andere bevoegde toezichthoudende autoriteit.

---

## ARTIKEL 2: DOEL, AARD EN GRONDSLAG

2.1. Noveu verwerkt de Persoonsgegevens uitsluitend in opdracht van Opdrachtgever en voor de uitvoering van de Hoofdovereenkomst, nimmer voor eigen doeleinden.

2.2. De verwerking heeft betrekking op de volgende doeleinden:

- (a) leveren en beheren van het SaaS-platform (Noveu Workspace); voor NoveuFlow, een WordPress-plugin op de website van Opdrachtgever, uitsluitend licentiebeheer, updates en support. Gegevens van klanten van Opdrachtgever in NoveuFlow blijven op die website en worden in het kader van NoveuFlow niet door Noveu verwerkt, behalve wat Opdrachtgever zelf in een supportticket opneemt (dat valt onder (g)); neemt Opdrachtgever de hosting van die website bij Noveu af, dan valt die verwerking onder (c). AI-functies van NoveuFlow koppelt Opdrachtgever zelf, met een eigen sleutel, en lopen niet via Noveu;
- (b) hosten, verzenden en opslaan van e-mailberichten en bijlagen;
- (c) web- en applicatiehosting;
- (d) beheer en beveiliging van de IT-infrastructuur van Opdrachtgever;
- (e) afspraken, agenda, contacten, CRM- en projectgegevens;
- (f) back-up en continuïteit;
- (g) support en helpdesk (ticketing);
- (h) optioneel: AI-ondersteunde functies (alleen na expliciete activering door Opdrachtgever).

2.3. Opdrachtgever garandeert dat de verwerking op een geldige grondslag in de zin van artikel 6 AVG berust en dat Persoonsgegevens rechtmatig zijn verkregen.

2.4. De aard en duur van de verwerking komen overeen met de duur van de Hoofdovereenkomst, vermeerderd met de in artikel 11 genoemde retentietermijnen.

---

## ARTIKEL 3: CATEGORIEËN PERSOONSGEGEVENS

3.1. In het kader van de Diensten kunnen de volgende categorieën Persoonsgegevens worden verwerkt:

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

| Categorie | Voorbeelden |
|---|---|
| Contactgegevens | naam, e-mail, telefoon, adres |
| Accountgegevens | gebruikersnaam, gehasht wachtwoord, rollen, MFA-secret |
| Communicatiegegevens | e-mailinhoud, bijlagen, chat-/berichtinhoud, metadata |
| Agenda- en afspraakgegevens | agenda-items, beschikbaarheid, deelnemers |
| CRM-/relatiegegevens | klantdossiers, notities, communicatiehistorie |
| Bestanden | documenten die Opdrachtgever uploadt of opslaat |
| Technische gegevens | IP-adressen, logs, device-info, sessiedata |
| Facturatiegegevens | factuuradres, BTW, IBAN (via Stripe) |
| Bijzondere categorieën (art. 9 AVG) | uitsluitend indien uitdrukkelijk overeengekomen en met aanvullende maatregelen (zie 3.3) |

3.2. **Categorieën betrokkenen:**

- (a) medewerkers en personeel van Opdrachtgever;
- (b) klanten en relaties van Opdrachtgever;
- (c) leveranciers en zakenpartners van Opdrachtgever;
- (d) bezoekers van websites van Opdrachtgever;
- (e) patiënten/cliënten (alleen in zorgcontext, zie 3.3);
- (f) sollicitanten.

3.3. **Bijzondere categorieën en zorgcontext (NTA 7516).** Indien de verwerking betrekking heeft op bijzondere persoonsgegevens (art. 9 AVG), waaronder gezondheidsgegevens:

- (a) Opdrachtgever informeert Noveu hier uitdrukkelijk en vooraf over;
- (b) Partijen treffen aanvullende maatregelen conform Bijlage 1;
- (c) Voor e-mail in de zorg past Noveu (indien overeengekomen) de normen van **NTA 7516 (Veilige e-mail in de zorg)** toe;
- (d) Opdrachtgever waarborgt een geldige grondslag conform artikel 9 lid 2 AVG.

---

## ARTIKEL 4: VERPLICHTINGEN VAN DE VERWERKER

4.1. Noveu verwerkt de Persoonsgegevens uitsluitend op basis van Schriftelijke instructies van Opdrachtgever, tenzij verplicht op grond van Unierecht of Nederlands recht. In dat geval informeert Noveu Opdrachtgever vooraf, tenzij de wet dat verbiedt.

4.2. Noveu verwerkt Persoonsgegevens niet buiten de EER, tenzij Opdrachtgever daarvoor Schriftelijke toestemming heeft gegeven en passende waarborgen (hoofdstuk V AVG) zijn getroffen.

4.3. Noveu informeert Opdrachtgever onverwijld indien een instructie naar het oordeel van Noveu in strijd is met de AVG of andere privacywetgeving.

4.4. Noveu verleent redelijke medewerking bij DPIA's (art. 35 AVG) en voorafgaande raadpleging (art. 36 AVG).

4.5. Noveu houdt een register van verwerkingsactiviteiten bij conform artikel 30 lid 2 AVG.

---

## ARTIKEL 5: BEVEILIGING (TOM's)

5.1. Noveu treft passende technische en organisatorische maatregelen conform artikel 32 AVG, rekening houdend met de stand van de techniek.

5.2. Een gedetailleerd overzicht van de TOM's is opgenomen in **Bijlage 1**. Op hoofdlijnen treft Noveu ten minste:

- (a) TLS 1.2+ voor extern verkeer, HSTS, moderne ciphers;

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

- (b) back-ups worden sinds 30 september 2026 versleuteld opgeslagen; de schijven zelf zijn nog niet versleuteld en een datum daarvoor geven we nog niet;
- (c) RBAC met least-privilege principe;
- (d) verplichte MFA voor alle beheertoegang;
- (e) centrale logging, monitoring (Prometheus/Grafana) en errortracking (GlitchTip);
- (f) dagelijkse geautomatiseerde back-ups. Back-ups staan in het Hetzner-datacenter in Falkenstein (Duitsland). Back-ups worden sinds 30 september 2026 versleuteld opgeslagen; de schijven zelf zijn nog niet versleuteld en een datum daarvoor geven we nog niet; periodieke hersteltests worden geïmplementeerd zodra de eerste productie-klanten zijn aangesloten;
- (g) patchmanagement (kritieke CVE's binnen 48 uur);
- (h) Cloudflare Tunnel voor het HTTP-verkeer, geen directe inbound internettoegang tot de web-backend (mailverkeer en STUN/TURN lopen rechtstreeks naar onze server bij Hetzner in Falkenstein, Duitsland, niet via Cloudflare);
- (i) segmentatie van omgevingen en data-isolatie per service.

5.3. Noveu evalueert deze maatregelen periodiek en past ze aan de stand van de techniek aan. Wezenlijke wijzigingen worden aan Opdrachtgever medegedeeld.

---

## ARTIKEL 6: SUB-VERWERKERS

6.1. Opdrachtgever geeft Noveu hierbij **algemene toestemming** voor het inschakelen van Sub-verwerkers, onder de voorwaarden van dit artikel.

6.2. De op het moment van publicatie ingeschakelde Sub-verwerkers staan in **Bijlage 2** en op /juridisch/sub-verwerkers. Opdrachtgever stemt daarmee in.

6.3. Noveu kondigt voorgenomen wijzigingen (toevoeging of vervanging) **minimaal 30 dagen** vooraf Schriftelijk aan, onder andere via e-mail en `https://noveu.eu/juridisch/sub-verwerkers`.

6.4. Opdrachtgever mag binnen die termijn gemotiveerd bezwaar maken. Leidt overleg niet binnen 14 dagen tot overeenstemming, dan mag Opdrachtgever de Hoofdovereenkomst opzeggen met 30 dagen opzegtermijn, zonder schadevergoeding.

6.5. Noveu legt aan iedere Sub-verwerker ten minste gelijkwaardige verplichtingen op en blijft jegens Opdrachtgever volledig aansprakelijk voor nakoming door Sub-verwerkers.

---

## ARTIKEL 7: MELDPLICHT DATALEKKEN

7.1. Noveu informeert Opdrachtgever zonder onredelijke vertraging en uiterlijk binnen **48 uur** na ontdekking van een Datalek, zodat Opdrachtgever tijdig kan voldoen aan de wettelijke meldplicht aan de AP (72 uur, art. 33 AVG).

7.2. De melding bevat ten minste, voor zover op dat moment bekend:

- (a) aard van het Datalek, categorieën en geschat aantal betrokkenen en Persoonsgegevens;
- (b) contactgegevens van de functionaris/contactpersoon bij Noveu;
- (c) waarschijnlijke gevolgen;
- (d) reeds genomen en voorgestelde maatregelen.

7.3. Ontbrekende informatie wordt in fasen aangevuld.

7.4. Noveu documenteert alle Datalekken in een intern register (art. 33 lid 5 AVG) en stelt dit op verzoek beschikbaar.

7.5. Noveu verleent redelijke medewerking aan Opdrachtgever bij: beperken van gevolgen, onderzoek, meldingen aan de Toezichthouder en/of betrokkenen (art. 33 tot en met 34 AVG), en vervolgvragen van de Toezichthouder.

7.6. Noveu doet zonder Schriftelijke toestemming geen mededelingen aan derden over een Datalek, tenzij wettelijk verplicht.

---

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

## ARTIKEL 8: RECHTEN VAN BETROKKENEN (DSR-BIJSTAND)

8.1. Opdrachtgever is zelf verantwoordelijk voor het afhandelen van verzoeken van betrokkenen (art. 15 tot en met 22 AVG): inzage, rectificatie, wissing, beperking, dataportabiliteit, bezwaar en geautomatiseerde besluitvorming.

8.2. Noveu ondersteunt Opdrachtgever binnen een termijn van **30 dagen** na ontvangst van een Schriftelijk verzoek, tenzij een kortere termijn redelijkerwijs noodzakelijk is om binnen wettelijke termijnen te blijven.

8.3. Ontvangt Noveu rechtstreeks een verzoek van een betrokkene, dan stuurt zij dit zo spoedig mogelijk door aan Opdrachtgever zonder inhoudelijk te reageren, tenzij Schriftelijk anders overeengekomen.

8.4. Redelijke kosten voor ondersteuning kunnen in rekening worden gebracht tegen Noveu's alsdan geldende tarief, mits vooraf gecommuniceerd.

---

## ARTIKEL 9: GEHEIMHOUDING

9.1. Noveu verplicht zich tot geheimhouding van alle Persoonsgegevens en overige vertrouwelijke informatie.

9.2. Noveu waarborgt dat alle personen die onder haar gezag handelen en toegang hebben tot Persoonsgegevens (werknemers, inhuurkrachten en freelancers) gebonden zijn aan een wettelijke of contractuele geheimhoudingsverplichting.

9.3. De geheimhouding blijft na beëindiging van kracht voor onbepaalde tijd of zolang de vertrouwelijkheid dit vereist.

---

## ARTIKEL 10: AUDIT

10.1. Noveu stelt Opdrachtgever alle redelijkerwijs benodigde informatie ter beschikking om naleving van artikel 28 AVG aan te tonen.

10.2. Opdrachtgever heeft het recht **eenmaal per kalenderjaar** een audit te (laten) uitvoeren, onder de volgende voorwaarden:

- (a) Schriftelijke aankondiging ten minste 20 werkdagen vooraf;
- (b) tijdens reguliere kantooruren, op afspraak;
- (c) met inachtneming van de vertrouwelijkheid van andere klanten;
- (d) door een onafhankelijke, gekwalificeerde auditor onder geheimhouding.

10.3. Aanvullende audits zijn toegestaan bij: een Datalek (art. 7), onderzoek door de Toezichthouder, of gegronde redenen om non-conformiteit te vermoeden.

10.4. Noveu mag in plaats van een fysieke audit een recent (max 12 maanden oud) extern auditrapport, ISO 27001 / SOC 2 / ISAE 3402 certificering of gelijkwaardige onafhankelijke verklaring aanbieden. Een fysieke audit is alleen toegestaan indien de aangeboden documentatie ontoereikend is.

10.5. Audits geschieden op kosten van Opdrachtgever, tenzij hieruit blijkt dat Noveu niet aan haar verplichtingen voldoet; dan draagt Noveu de redelijke kosten.

10.6. Noveu werkt mee aan onderzoeken door de Toezichthouder voor zover deze betrekking hebben op deze DPA.

---

## ARTIKEL 11: TERUGGAVE EN VERWIJDERING

11.1. Bij beëindiging van de Hoofdovereenkomst staakt Noveu de verwerking, behoudens wettelijke bewaarplichten.

11.2. Op verzoek van Opdrachtgever stelt Noveu de Persoonsgegevens in een gangbaar en machineleesbaar formaat (CSV, JSON, SQL-export, MBOX voor mail) **binnen 30 dagen** ter beschikking. Opdrachtgever heeft **30 dagen** na beëindiging om een verzoek tot teruggave in te dienen.

11.3. Na teruggave, of na afloop van de termijn in 11.2 zonder verzoek, verwijdert Noveu alle Persoonsgegevens en kopieën **binnen 30 dagen**.

11.4. **Back-ups** met Persoonsgegevens worden uiterlijk **90 dagen** na beëindiging overschreven of verwijderd. Gedurende die periode blijven de beveiligings- en geheimhoudingsverplichtingen onverminderd gelden.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

11.5. Noveu bevestigt de verwijdering Schriftelijk op verzoek.

---

## ARTIKEL 12: AANSPRAKELIJKHEID

12.1. Opdrachtgever is en blijft verantwoordelijk voor de naleving van de AVG met betrekking tot de verwerking waarvoor zij verantwoordelijke is.

12.2. Noveu is aansprakelijk voor schade voor zover zij:

- (a) niet heeft voldaan aan de specifiek tot verwerkers gerichte AVG-verplichtingen; of
- (b) in strijd heeft gehandeld met rechtmatige instructies van Opdrachtgever; of
- (c) buiten of in strijd met de instructies heeft gehandeld.

12.3. Een Partij is vrijgesteld van aansprakelijkheid wanneer zij bewijst op geen enkele wijze verantwoordelijk te zijn voor het schadeveroorzakende feit (art. 82 lid 3 AVG).

12.4. De aansprakelijkheidsbeperkingen uit de Algemene Voorwaarden (artikel 13) zijn van overeenkomstige toepassing, met dien verstande dat deze niet gelden bij dwingendrechtelijke AVG-aansprakelijkheid of bij schending van de geheimhoudingsplicht (artikel 9).

12.5. Indien een betrokkene schade claimt, stellen Partijen elkaar onverwijld op de hoogte en werken zij redelijk samen bij de afhandeling. Indien de ene Partij schadevergoeding betaalt, mag zij het deel dat overeenkomt met de verantwoordelijkheid van de andere Partij terugvorderen.

---

## ARTIKEL 13: LOOPTIJD EN SLOTBEPALINGEN

13.1. Deze DPA treedt in werking bij het sluiten van de Hoofdovereenkomst en eindigt van rechtswege bij beëindiging daarvan. Bepalingen die naar hun aard voortduren (geheimhouding, verwijdering, aansprakelijkheid) blijven van kracht.

13.2. Wijzigingen en aanvullingen zijn slechts geldig indien Schriftelijk overeengekomen.

13.3. Bij strijdigheid met de Hoofdovereenkomst prevaleert deze DPA voor zover het de verwerking van Persoonsgegevens betreft.

13.4. Op deze DPA is **Nederlands recht** van toepassing. Geschillen worden voorgelegd aan de **Rechtbank Den Haag**, onverminderd het recht van Partijen op mediation of arbitrage.

13.5. De kernverwerking en -opslag van Persoonsgegevens vindt plaats binnen de EER. Voor de met name genoemde sub-verwerkers buiten de EER (zie Bijlage 2) zijn passende waarborgen getroffen conform hoofdstuk V AVG (EU-VS Data Privacy Framework en/of Standard Contractual Clauses, zoals per sub-verwerker vermeld in Bijlage 2). Wijzigingen in deze waarborgen of in de lijst van niet-EER-sub-verwerkers worden conform artikel 6 vooraf aangekondigd.

---

## ONDERTEKENING

Aldus overeengekomen:

**Verwerkingsverantwoordelijke:**

| | |
|---|---|
| Naam | `[Naam vertegenwoordiger]` |
| Functie | `[Functie]` |
| Datum | `[Datum]` |
| Handtekening | _____ |

**Verwerker (Noveu Solutions):**

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

| | |
|---|---|
| Naam | M. de Visser |
| Functie | Eigenaar |
| Datum | `[Datum]` |
| Handtekening | _____ |

## BIJLAGE 1: TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

### A. Infrastructuur en netwerk

| Maatregel | Specificatie |
|---|---|
| Primaire hostinglocatie | Hetzner Dedicated, Falkenstein (Duitsland), eigen ijzer, Proxmox VE |
| Back-uplocatie | Back-ups staan in het Hetzner-datacenter in Falkenstein (Duitsland). Back-ups worden sinds 30 september 2026 versleuteld opgeslagen. De schijven zelf zijn nog niet versleuteld; een datum daarvoor geven we nog niet. |
| Mail-infrastructuur | Stalwart mailserver op vm-mail (10.10.10.11): EU-gehost |
| Edge/DDoS | Cloudflare (wereldwijd netwerk): DDoS-mitigatie, WAF, DNSSEC |
| Inbound-architectuur | HTTP-verkeer via **Cloudflare Tunnel** (web-backend zonder publieke poort); mailverkeer (protocollen SMTP, IMAP en JMAP) en STUN/TURN rechtstreeks naar de eigen server bij Hetzner in Falkenstein, niet via Cloudflare |
| Netwerksegmentatie | Docker-netwerken per service; alleen API-gateway extern bereikbaar |
| Firewall | Host-firewall + Proxmox/VM-firewall; whitelisting |

### B. Applicatiebeveiliging

| Maatregel | Specificatie |
|---|---|
| Authenticatie | JWT + refresh tokens; Redis-gebacked sessies |
| MFA | TOTP verplicht voor alle beheer- en admin-accounts |
| Autorisatie | RBAC met granulaire rechten per service |
| API-gateway | Rate limiting, input-validatie, CORS, auth-header-propagatie |
| Wachtwoordopslag | bcrypt / Argon2, nooit plaintext |
| TLS | TLS 1.2+ verplicht, HSTS, moderne ciphers |

### C. E-mailbeveiliging

| Maatregel | Specificatie |
|---|---|
| Transport | STARTTLS verplicht; MTA-STS ingeschakeld |
| Authenticatie | SPF, DKIM, DMARC per domein; ARC voor forwarding |
| Spamfilter | Actieve spam- en malwarefiltering (Stalwart) |
| NTA 7516 | Optioneel voor zorgklanten, afzonderlijk overeengekomen |

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

### D. Gegevensbeheer

| Maatregel | Specificatie |
|---|---|
| Encryptie-at-rest | De schijven zelf zijn nog niet versleuteld; een datum daarvoor geven we nog niet. Back-ups worden sinds 30 september 2026 versleuteld opgeslagen. Encryptie in transit: TLS 1.2 of hoger, TLS 1.3 wordt ondersteund. |
| Data-isolatie | Eigen schema per service; logische scheiding per tenant/organisatie |
| Back-ups | Dagelijks geautomatiseerd, retentie 30 dagen (periodieke hersteltests worden geïmplementeerd na eerste productie-klant) |
| Dataportabiliteit | Export in CSV, JSON, SQL en MBOX (mail) |
| Verwijdering | Geautomatiseerde wipe bij beëindiging (art. 11 DPA) |

### E. Toegangsbeheer en personeel

| Maatregel | Specificatie |
|---|---|
| Least-privilege | Productietoegang alleen voor geautoriseerde engineers |
| MFA beheer | Verplicht voor SSH, Proxmox, Portainer, Grafana, databases |
| Logging | Admin-toegang + wijzigingen gelogd; centraal opgeslagen |
| NDA | Alle medewerkers en inhuurkrachten tekenen NDA |
| Offboarding | Toegangsrechten ingetrokken binnen 24 uur na uitdiensttreding |

### F. Monitoring en incident response

| Maatregel | Specificatie |
|---|---|
| Monitoring | Prometheus + Grafana (vm-monitoring) |
| Error tracking | GlitchTip ( `errors.noveu.eu` ) |
| Detectie | Geautomatiseerde alerts op anomalieën en failures |
| Datalekmelding | Binnen 48 uur aan Opdrachtgever (art. 7 DPA) |
| Incidentregister | Alle incidenten gedocumenteerd en periodiek geëvalueerd (RCA) |

### G. Organisatorisch

| Maatregel | Specificatie |
|---|---|
| Beveiligingsbeleid | Gedocumenteerd intern security-beleid |
| Bewustwording | Periodieke security-training voor medewerkers |
| Leveranciersbeheer | Sub-verwerkers gescreend en contractueel gebonden |
| Change management | Wijzigingen via versiebeheer (Git) + review |

---

## BIJLAGE 2: OVERZICHT SUB-VERWERKERS

Actuele stand op moment van publicatie. Een actueel overzicht is raadpleegbaar op /juridisch/sub-verwerkers.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

| # | Sub-verwerker | Vestiging | Verwerkingslocatie | Doel/Dienst | Categorieën gegevens | Waarborg |
|---|---|---|---|---|---|---|
| 1 | **Hetzner Online GmbH** | Duitsland (EU) | Falkenstein (DE) | Dedicated server, storage en back-ups | Alle categorieën art. 3 | AVG: EU-entiteit |
| 2 | **Cloudflare, Inc.** | VS (EU-entity beschikbaar) | Wereldwijd netwerk van Cloudflare, zonder beperking tot de EU | CDN, DDoS, DNS, Tunnel | IP-adressen, metadata, TLS-terminatie | EU-VS DPF + SCC's + DPA |
| 3 | **Stripe Payments Europe Ltd.** | Ierland (EU) | EU | Betalingsverwerking (kaarten, iDEAL, SEPA) | Facturatie-, bedrijfs- en betaalgegevens | AVG: EU-entiteit + DPA |
| 4 | **Mistral AI SAS** | Frankrijk (EU) | EU | AI-functionaliteit (Noveu AI), **alleen LLM-tekstgeneratie**, uitsluitend bij expliciete activering. Embeddings worden **niet** naar Mistral verstuurd; deze draaien on-premise (zie zelf-gehoste infrastructuur hieronder). | Alleen content die gebruiker aan AI aanbiedt | AVG: EU-entiteit + Mistral DPA + data-minimisatie/pseudonimisatie in de Noveu AI-gateway |

**Uitgefaseerd:**

| Sub-verwerker | Rol | Uitgefaseerd per |
|---|---|---|
| **Google LLC (Gemini API)** | AI, LLM-tekstgeneratie | 29 augustus 2026 |

**Opmerkingen:**

- De AI-verwerker (Mistral AI SAS, Parijs) wordt **uitsluitend** ingezet na expliciete activering per feature en **enkel voor LLM-tekstgeneratie**. Alleen door de gebruiker aangeboden content wordt verstuurd; deze betalende API-laag traint niet op klantdata. De **embeddings (vectorisatie) en de vector-store zijn self-hosted** (BAAI `bge-m3` via zelf-gehoste Text-Embeddings-Inference + pgvector op eigen Hetzner-infra, EU); er wordt geen externe embedding-API of externe vector-database gebruikt. Anthropic, OpenAI, Google en Pinecone zijn **niet** in gebruik.
- **Wijziging AI-verwerker.** Google LLC (Gemini API, VS) is per 29 augustus 2026 vervangen door Mistral AI SAS (Frankrijk, EU-verwerking). De aankondiging conform artikel 6.3 is gepubliceerd op 31 augustus 2026 op /juridisch/sub-verwerkers; de bezwaartermijn loopt tot en met 31 oktober 2026, gelijk aan de sub-verwerkerspagina. De omschakeling verplaatst de AI-verwerking van buiten naar binnen de EER en voegt geen sub-verwerker toe.
- Voor VS-verwerkers zijn aanvullende maatregelen getroffen conform Schrems II (SCC's, data-minimisatie, encryptie in transit via TLS 1.2 of hoger, US CLOUD Act-risicoanalyse). Na de wijziging hierboven is Cloudflare de enige resterende sub-verwerker met een VS-nexus.
- Een detail-overzicht inclusief links naar sub-verwerker-DPA's staat op /juridisch/sub-verwerkers.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

## BIJLAGE 3: VERWERKINGSACTIVITEITEN

| # | Activiteit | Categorieën gegevens | Betrokkenen | Bewaartermijn |
|---|---|---|---|---|
| 1 | Noveu Workspace (SaaS) | Contact-, account-, CRM-, agenda-, bestand- en communicatiegegevens | Medewerkers, klanten, relaties | Duur overeenkomst + 30 dagen |
| 2 | NoveuFlow (WordPress-plugin): licentie, updates en support | Licentiesleutel, e-mailadres van de beheerder of licentiehouder, domein en site-URL, pluginversie en tijdstempels; bij een supportticket ook de vrije tekst, WordPress-, PHP- en pluginversie, plan en sector. De plugin stuurt zelf geen gegevens van klanten van Opdrachtgever mee; wat de beheerder zelf in een supportticket zet, valt onder rij 6 | Beheerder of licentiehouder van Opdrachtgever | Licentie- en updategegevens: duur licentie + 30 dagen; supporttickets: 24 maanden na sluiten ticket (rij 6) |
| 3 | Mail Hosting (Stalwart) | Communicatiegegevens, contactgegevens, metadata | Medewerkers, klanten, relaties | Duur overeenkomst + 30 dagen |
| 4 | Webhosting | Websitegegevens, technische gegevens | Websitebezoekers | Duur overeenkomst + 30 dagen |
| 5 | Managed IT-diensten | Account- en technische gegevens | Medewerkers | Duur overeenkomst + 30 dagen |
| 6 | Support/ticketing | Contact- en communicatiegegevens | Medewerkers, klanten | 24 maanden na sluiten ticket |
| 7 | Betalingsverwerking (Stripe) | Factuur- en betaalgegevens | Contactpersonen | Fiscale bewaartermijn 7 jaar |
| 8 | AI-diensten (optioneel) | Inhoud door gebruiker aangeboden; afgeleide embeddings | Afhankelijk van gebruik | Mistral (LLM-tekst, EU) traint niet op klantdata; afgeleide embeddings worden lokaal gegenereerd (on-premise) en opgeslagen in de self-hosted EU vector-store (pgvector) zolang de AI-functie actief is |
| 9 | Back-ups | Alle bovengenoemde categorieën | Alle bovengenoemde | Maximaal 90 dagen na beëindiging |
| 10 | Error-/monitoringlogs | Technische gegevens, event-IDs | Gebruikers | 30 dagen |

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

## CHANGELOG

| Versie | Datum | Wijziging |
|---|---|---|
| 1.9.1 | 21 oktober 2026 | Feitelijke correctie: Mollie B.V. is geen sub-verwerker of betaaldienstverlener van Noveu en is verwijderd. Gewijzigd zijn Artikel 3.1 (rij Facturatiegegevens: betalingen lopen alleen via Stripe), Bijlage 2 (rij 4, Mollie B.V., vervalt; Mistral AI SAS is nu rij 4; bij Stripe staat iDEAL nu als betaalmethode genoemd, gelijk aan de algemene voorwaarden) en Bijlage 3 (rij 7, Betalingsverwerking: alleen Stripe). De overige onderdelen zijn ongewijzigd. |
| 1.9 | 14 oktober 2026 | Feitelijke correctie. Back-ups worden sinds 30 september 2026 versleuteld opgeslagen. De schijven zelf zijn nog niet versleuteld; een datum daarvoor geven we nog niet. De eerder geplande datum voor versleuteling van de schijven is vervallen. Gewijzigd zijn artikel 5.2 (maatregelen b en f), Bijlage 1 A (back-uplocatie) en Bijlage 1 D (gegevensbeheer). De bewaartermijnen en de overige artikelen en bijlagen zijn ongewijzigd. |
| 1.8 | 7 oktober 2026 | Feitelijke correctie naar de gemeten stand van 30 september 2026: back-ups worden sinds 30 september 2026 versleuteld opgeslagen. Versleuteling van overige opslag at rest wordt ingevoerd (gepland oktober 2026). Gewijzigd zijn artikel 5.2 (maatregelen b en f), Bijlage 1 A (back-uplocatie) en Bijlage 1 D (gegevensbeheer). De bewaartermijnen en de overige artikelen en bijlagen zijn ongewijzigd. |
| 1.7 | 30 september 2026 | Feitelijke correctie naar de meting van 30 september 2026: correctie van de beschrijving van Cloudflare en van de mail- en STUN/TURN-diensten. Bijlage 1 A en Bijlage 2 (rij 2) noemden EU-datacenters; Cloudflare verwerkt het verkeer in zijn wereldwijde netwerk, zonder beperking tot de EU. Bijlage 1 A (inbound-architectuur): mailverkeer en STUN/TURN lopen rechtstreeks naar de eigen server bij Hetzner in Falkenstein, niet via Cloudflare. Bijlage 1 D en Bijlage 2 (opmerkingen): encryptie in transit is TLS 1.2 of hoger, TLS 1.3 wordt ondersteund. Art. 5.2(h) noemde de mail- en STUN/TURN-poorten gehard; dat was niet gemeten en is geschrapt. Geen nieuwe of vervangen sub-verwerker en geen wijziging van de verplichtingen. |
| 1.6 | 29 september 2026 | Feitelijke correctie naar de gemeten stand van 29 september 2026. Gewijzigd zijn artikel 5.2 (maatregelen b en f), Bijlage 1 A (back-uplocatie) en Bijlage 1 D (gegevensbeheer). Bijlage 1 A noemde versleutelde back-ups als actief, maar er waren toen geen versleutelde back-ups. De nieuwe tekst op die plekken: back-ups staan in het Hetzner-datacenter in Falkenstein (Duitsland); versleuteling van back-ups en opslag at rest wordt ingevoerd (gepland oktober 2026). Regel 1.4 is geannoteerd als onjuist. Behalve de hier genoemde onderdelen zijn de artikelen en bijlagen ongewijzigd. |
| 1.5 | 28 september 2026 | Bijlage 2 (opmerking "Wijziging AI-verwerker"): de bezwaartermijn voor de wisseling van Google LLC naar Mistral AI SAS loopt tot en met 31 oktober 2026 in plaats van 30 september 2026, gelijk aan de sub-verwerkerspagina (versie 1.4). Behalve deze opmerking zijn de artikelen en bijlagen ongewijzigd. |
| 1.4 | 28 september 2026 | Artikel 5 (maatregel f), Bijlage 1 (back-uplocatie) en Bijlage 2 (rij 1, Hetzner): datalocatie gecorrigeerd naar de gemeten stand van 26 september 2026. Gegevens en versleutelde back-ups staan in een Hetzner-datacenter in Falkenstein (Duitsland); de eerdere vermelding van een aparte back-uplocatie en van replicatie naar een andere locatie is verwijderd. Geen nieuwe of vervangen sub-verwerker; het aantal actieve sub-verwerkers blijft vijf. In de historische regel van versie 1.0 is de naam van de vroegere back-uplocatie vervangen door een omschrijving. Overweging A, artikel 2.2(a) en Bijlage 3 (rij 2, NoveuFlow): NoveuFlow is een WordPress-plugin op de website van Opdrachtgever; Noveu verwerkt daarvoor alleen licentie-, update- en supportgegevens en geen gegevens van klanten van Opdrachtgever. Behalve de hier genoemde onderdelen zijn de artikelen en bijlagen ongewijzigd. (onjuist; gecorrigeerd in v1.6) |

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.

| | | |
|---|---|---|
| 1.3 | 31 augustus 2026 | **Wisseling AI-sub-verwerker doorgevoerd in Bijlage 2 en Bijlage 3.** Google LLC (Gemini API, VS) is vervangen door Mistral AI SAS (Frankrijk, verwerking binnen de EU). De technische omschakeling vond plaats op 29 augustus 2026; de aankondiging conform artikel 6.3 is op 31 augustus 2026 gepubliceerd op /juridisch/sub-verwerkers, met een bezwaartermijn tot en met 30 september 2026. De documenten liepen tot deze versie achter op de werkelijkheid: zij noemden Google als huidige AI-verwerker en Mistral als roadmap-optie. Concreet gewijzigd: (a) Bijlage 2 rij 5 vervangen; (b) een rubriek "Uitgefaseerd" toegevoegd met Google en de datum 29 augustus 2026; (c) de opmerking onder Bijlage 2 herschreven, inclusief de vaststelling dat Cloudflare na deze wijziging de enige resterende sub-verwerker met VS-nexus is; (d) Bijlage 3 rij 8 (AI-diensten) van Google naar Mistral. Geen wijziging in de categorieën gegevens, de bewaartermijnen of de rest van de overeenkomst. |
| 1.2 | 5 juli 2026 | Correctie artikel 13.5: de bepaling stelde dat verwerkingen **uitsluitend binnen de EER** plaatsvinden en dat geen SCC's nodig zijn, terwijl Bijlage 2 voor Cloudflare (VS) en Google/Gemini (VS) juist **EU-VS DPF + SCC's** als waarborg vermeldt. Artikel 13.5 luidt nu: kernverwerking en -opslag binnen de EER; voor de in Bijlage 2 genoemde niet-EER-sub-verwerkers gelden passende waarborgen conform hoofdstuk V AVG (DPF en/of SCC's); wijzigingen worden conform artikel 6 vooraf aangekondigd. Geen wijziging in de feitelijke verwerking, uitsluitend het in lijn brengen van artikel 13.5 met de reeds gepubliceerde Bijlage 2. |
| 1.1 | 16 juni 2026 | Correctie sub-verwerkerslijst naar de feitelijke productie-stand: de enige externe AI-verwerker is **Google (Gemini API)**, uitsluitend voor **LLM-tekstgeneratie**. **Anthropic en OpenAI zijn verwijderd**: niet in gebruik. **Embeddings en vector-store zijn self-hosted/on-premise** (BAAI `bge-m3` via zelf-gehoste Text-Embeddings-Inference + pgvector op eigen Hetzner-EU-infra); géén externe embedding-API en géén externe vector-database (Pinecone niet in gebruik). Bijlage 3 "Zero-retention (geen opslag)" voor AI gecorrigeerd: afgeleide embeddings worden lokaal opgeslagen in de self-hosted EU vector-store. Mistral (Parijs) genoemd als EU-soevereine roadmap-optie, niet als huidige stand. |
| 1.0 | 9 juni 2026 | Eerste publicatie-klare versie, gebaseerd op interne template (NLdigital-basis). Wijzigingen t.o.v. template: (a) sub-verwerkerslijst volledig bijgewerkt: Strato vervangen door Hetzner (Falkenstein plus een aparte back-uplocatie; per versie 1.4 gecorrigeerd), Stripe en Mollie expliciet, Anthropic toegevoegd als primaire AI, OpenAI als optioneel alternatief (Bijlage 2); (b) TOM's uitgebreid met actuele Noveu-infra: Cloudflare Tunnel, Stalwart, Proxmox, Prometheus/Grafana, GlitchTip (Bijlage 1); (c) datalekmeldtermijn aangepast naar 48 uur (art. 7); (d) DSR-bijstand termijn expliciet op 30 dagen (art. 8); (e) audit-regime verduidelijkt, 1x/jaar op afspraak, ISO/SOC2-rapport aanvaardbaar (art. 10); (f) NTA 7516 expliciet benoemd als optioneel voor zorgklanten (art. 3.3); (g) toegevoegd: verwerkingen uitsluitend binnen EER, geen SCC's nodig (art. 13.5); (h) NL-forum vastgelegd op Rechtbank Den Haag (art. 13.4); (i) Bijlage 3 bewaartermijnen concreet gemaakt (support 24m, errorlogs 30d, AI zero-retention). |

***Gerelateerde documenten:***

- *Algemene Voorwaarden Noveu B2B, /juridisch/algemene-voorwaarden*
- *Privacyverklaring, /legal/privacy*
- *Actuele sub-verwerkers, /juridisch/sub-verwerkers*
- *Status- en incidentenpagina,* `https://status.noveu.eu`

**Conceptversie.** Deze DPA is in eindfase maar nog niet juridisch gecontroleerd voor ondertekening. Voor ondertekening door beide partijen is juridische review vereist.