VERWERKERSOVEREENKOMST — Vastly

Versie 1.2 — vastgesteld 5 oktober 2026 (v1.1: 24 september 2026; v1.0: 22 augustus 2026).

Partijen

1. **[KLANTNAAM]**, gevestigd te [adres], ingeschreven in het Handelsregister onder nummer [KvK-nummer], hierna: **"Verwerkingsverantwoordelijke"** of **"Klant"**;
2. **PDL Powerhouse B.V.**, handelend onder de naam **Vastly**, gevestigd te Arnhem aan de Turfstraat 1-3, 6811 HL, ingeschreven in het Handelsregister onder nummer 42063059, hierna: **"Verwerker"** of **"Vastly"**;

hierna gezamenlijk: **"Partijen"**.

Overwegingen

- De Klant neemt van Vastly de software-dienst Vastly af (vastgoedbeheer: contracten, facturatie, debiteuren en indexatie) op grond van een abonnementsovereenkomst, hierna: de **"Hoofdovereenkomst"**.
- Bij het gebruik van de dienst voert de Klant gegevens in over zijn huurders, contracten en objecten. Voor die gegevens is de Klant (verhuurder) verwerkingsverantwoordelijke en is Vastly verwerker — dezelfde rolverdeling als publiek beschreven in de privacyverklaring van Vastly (§2).
- Partijen leggen met deze verwerkersovereenkomst (hierna: **"VWO"**) hun afspraken vast als bedoeld in artikel 28 lid 3 van de Algemene verordening gegevensbescherming (**"AVG"**).
- Deze VWO is onderdeel van en accessoir aan de Hoofdovereenkomst; zij wordt bij het aangaan van de Hoofdovereenkomst (onboarding) gesloten en eindigt van rechtswege bij het einde daarvan, met inachtneming van artikel 14.
- **Rangorde:** bij strijdigheid tussen deze VWO en de Hoofdovereenkomst prevaleert deze VWO voor zover het de verwerking van persoonsgegevens betreft; voor al het overige prevaleert de Hoofdovereenkomst.

Artikel 1 — Definities

1.1 Begrippen uit de AVG ("persoonsgegevens", "verwerken", "betrokkene", "inbreuk in verband met persoonsgegevens" (datalek), "subverwerker", "toezichthoudende autoriteit") hebben in deze VWO de betekenis die de AVG daaraan geeft.

1.2 Aanvullend geldt:

- **"Dienst"**: de Vastly-software zoals omschreven in de Hoofdovereenkomst.
- **"Klantdata"**: alle persoonsgegevens die de Klant of diens gebruikers in het kader van de Dienst invoeren, uploaden of laten genereren en waarvoor de Klant verwerkingsverantwoordelijke is.
- **"Read-only-naperiode"**: de periode van **30 dagen** direct na de einddatum van de Hoofdovereenkomst, waarin de gebruikers van de Klant uitsluitend leestoegang hebben en de zelfservice-export beschikbaar blijft (artikel 14).
- **"Zelfservice-export"**: de door de Dienst geboden exportfunctie per verhuurder-entiteit (zip-bestand met contract-PDF's, factuur-PDF's en machineleesbare kerngegevens-JSON), doorlopend beschikbaar via "Mijn gegevens".

Artikel 2 — Voorwerp, duur, aard en doel van de verwerking

2.1 Verwerker verwerkt Klantdata uitsluitend ten behoeve van het leveren van de Dienst aan de Klant: het voeren van de huuradministratie (objecten, huurders, contracten), het genereren en verzenden van facturen en betalingsherinneringen namens de Klant, debiteurenbeheer, huurindexatie, documentbeheer (waaronder elektronische ondertekening) en de daarbij behorende opslag, back-up en beveiliging.

2.2 De verwerking duurt zolang de Hoofdovereenkomst loopt, verlengd met de Read-only-naperiode en het in artikel 14 omschreven verwijdertraject.

2.3 De aard van de verwerking is: opslaan, structureren, raadplegen, gebruiken, verstrekken door verzending (aan door de Klant aangewezen ontvangers, zoals huurders), en wissen. Verwerker verwerkt Klantdata niet voor eigen doeleinden, verkoopt geen persoonsgegevens en gebruikt Klantdata niet voor advertenties of het trainen van AI-modellen.

Artikel 3 — Categorieën betrokkenen en persoonsgegevens

3.1 **Categorieën betrokkenen:** huurders en medehuurders van de Klant; gebruikers van de Klant (eigenaren, kantoormedewerkers); contactpersonen van de Klant en van derden in het contractdossier.

3.2 **Categorieën persoonsgegevens** (conform privacyverklaring §3): NAW-gegevens van huurders, e-mailadres en telefoonnummer, geboortedatum (particuliere huurders, voor contracten), contract- en factuurgegevens, betalingsstatus, communicatie (verzonden facturen en herinneringen), en documenten in het contractdossier (huurcontracten, opleveringsdocumenten, identificatiegegevens bij elektronische ondertekening via de e-sign-subverwerker).

3.3 De Dienst is niet bedoeld voor bijzondere categorieën persoonsgegevens (art. 9 AVG) of gegevens over strafrechtelijke veroordelingen (art. 10 AVG); de Klant staat ervoor in deze niet in te voeren.

Artikel 4 — Instructies van de Verwerkingsverantwoordelijke

4.1 Verwerker verwerkt Klantdata uitsluitend op basis van schriftelijke instructies van de Klant, tenzij een Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot verwerking verplicht; in dat geval stelt Verwerker de Klant voorafgaand aan de verwerking in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

4.2 De Hoofdovereenkomst, deze VWO en de configuratie die de Klant binnen de Dienst zelf instelt (waaronder verzendschema's voor facturen en herinneringen en de aan/uit-stand van optionele functies) gelden als de volledige en schriftelijke instructie. De Dienst voert geen autonome uitgaande acties richting huurders en geen financiële transacties uit zonder door de Klant geconfigureerde of bevestigde opdracht (mens-in-de-lus als ontwerpprincipe).

4.3 Indien een instructie naar het oordeel van Verwerker in strijd is met de AVG of andere toepasselijke privacywetgeving, stelt Verwerker de Klant daarvan onverwijld in kennis en is Verwerker gerechtigd de uitvoering op te schorten totdat de instructie is aangepast of bevestigd.

Artikel 5 — Geheimhouding

5.1 Verwerker waarborgt dat de tot het verwerken van Klantdata gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

5.2 Toegang tot Klantdata is beperkt tot personen voor wie die toegang noodzakelijk is voor de uitvoering van de Dienst (least privilege); het toegangsmodel scheidt klantomgevingen en beheerstoegang (zie Bijlage 2).

Artikel 6 — Beveiliging (art. 32 AVG)

6.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. De op de ingangsdatum getroffen maatregelen zijn beschreven in **Bijlage 2**.

6.2 Verwerker mag de maatregelen actualiseren, mits het beveiligingsniveau per saldo niet verslechtert. Bij een materiële wijziging wordt Bijlage 2 bijgewerkt en de Klant geïnformeerd.

6.3 Partijen stellen vast dat de in Bijlage 2 beschreven maatregelen, rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, de omvang, de context en de doeleinden van de verwerking alsmede de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen, een passend beveiligingsniveau als bedoeld in art. 32 AVG waarborgen.

Artikel 7 — Subverwerkers en ontvangers

7.1 De Klant verleent Verwerker **algemene toestemming** voor het inschakelen van subverwerkers. De op de ingangsdatum ingeschakelde subverwerkers zijn opgenomen in **Bijlage 1**.

7.2 Verwerker legt aan iedere subverwerker bij overeenkomst verplichtingen inzake gegevensbescherming op die een **gelijkwaardig beschermingsniveau** waarborgen als de verplichtingen in deze VWO, in het bijzonder het bieden van afdoende garanties met betrekking tot passende technische en organisatorische maatregelen. Verwerker blijft jegens de Klant volledig aansprakelijk voor de nakoming van de verplichtingen van de subverwerker.

7.3 Verwerker informeert de Klant over een voorgenomen toevoeging of vervanging van een subverwerker. De Klant kan binnen **30 dagen** na die kennisgeving schriftelijk en gemotiveerd bezwaar maken. Partijen treden dan in overleg; leidt dat niet tot een oplossing, dan mag de Klant de Hoofdovereenkomst opzeggen tegen de datum waarop de wijziging ingaat.

7.4 **Ontvangers (zelfstandige verwerkingsverantwoordelijken).** Sommige door de Dienst ondersteunde diensten van derden zijn geen subverwerker maar zelfstandig verwerkingsverantwoordelijke voor hun eigen verwerking; zij vallen buiten Bijlage 1 en buiten de aansprakelijkheidsregel van 7.2. Dat geldt voor:

a. **Mollie B.V.** (Nederland): vergunninghoudende betaaldienstverlener (PSD2) voor betaallinks aan huurders; betalingen lopen rechtstreeks via het betaalaccount van de Klant. Mollie verwerkt de betaalgegevens onder eigen verantwoordelijkheid en eigen (wettelijke) verplichtingen. Mollie is daarnaast betaaldienstverlener voor de eigen verkopen van Verwerker (abonnementsfacturen aan de Klant, tegoed voor de huurprijscheck); daarbij verwerkt Mollie geen Klantdata;

b. **Online Payment Platform B.V.** (Nederland, vergunninghoudende betaalinstelling) voor de wettelijke klantidentificatie (KYC) van de Klant als sub-merchant en voor de uitbetaling aan de Klant: zelfstandig verwerkingsverantwoordelijke. Voor de verwerking van huurbetalingen die via de Dienst worden gestart (betaalgegevens van huurders) staat Online Payment Platform als subverwerker in Bijlage 1; en

c. een toekomstige **bankkoppeling** via een vergunninghoudende rekeninginformatiedienstverlener (AISP, PSD2): die treedt op onder eigen verantwoordelijkheid.

Verwerker benoemt zulke ontvangers wél in de actuele subverwerkersinformatie (opvraagbaar via info@vastly.software).

7.5 **Kennisgeving (v1.1).** Verwerker houdt de actuele subverwerkerslijst openbaar op vastly.software/privacy (punt 5) en in Bijlage 1. Een voorgenomen toevoeging of vervanging kondigt Verwerker ten minste **30 dagen** vóór inschakeling aan per e-mail aan het bij het account bekende adres van de Klant én in de Dienst; de bezwaartermijn van 7.3 loopt vanaf die kennisgeving. Bij een wijziging van de aard of locatie van de verwerking door een bestaande subverwerker (bijvoorbeeld een nieuwe verwerkingsregio of een gewijzigd doorgiftemechanisme) geldt dezelfde kennisgeving. De subverwerkers die in Bijlage 1 van deze versie 1.1 zijn toegevoegd ten opzichte van versie 1.0, waren vóór inwerkingtreding van deze versie al bekendgemaakt in de privacyverklaring op vastly.software/privacy (punt 5, stand 12 september 2026 en later); voor bestaande Klanten geldt de kennisgeving van versie 1.1 als kennisgeving in de zin van 7.3.

Artikel 8 — Doorgifte buiten de EER

8.1 Verwerking van Klantdata vindt plaats binnen de Europese Economische Ruimte; de applicatie, database en documentopslag draaien in Google Cloud-regio **europe-west4 (Nederland)**.

8.2 Voor zover een subverwerker persoonsgegevens buiten de EER verwerkt of daartoe toegang heeft, draagt Verwerker zorg voor een geldig doorgiftemechanisme als bedoeld in hoofdstuk V AVG. Voor de subverwerkers **Google Cloud EMEA Limited** en **Expo** geldt als basis hun certificering onder het **EU-U.S. Data Privacy Framework** (adequaatheidsbesluit, art. 45 AVG); komt die certificering of het adequaatheidsbesluit te vervallen, dan gelden de door de Europese Commissie vastgestelde **standaardcontractsbepalingen (SCC's, art. 46 AVG)** als terugvalmechanisme. Aanvullende technische waarborg is de versleuteling at rest met door Verwerker beheerde sleutels (CMEK, Bijlage 2).

Artikel 9 — Bijstand bij rechten van betrokkenen

9.1 Verwerker verleent de Klant, rekening houdend met de aard van de verwerking, bijstand bij het vervullen van diens plicht om verzoeken van betrokkenen (inzage, rectificatie, verwijdering, beperking, overdraagbaarheid, bezwaar) te beantwoorden.

9.2 Die bijstand verloopt in de eerste plaats via de **zelfservicefunctionaliteit** van de Dienst, waaronder de Zelfservice-export: per verhuurder-entiteit, doorlopend beschikbaar (maximaal één export per entiteit per dag), met een machineleesbaar kerngegevensdeel (JSON) dat geschikt is voor art.-20-verzoeken.

9.3 Ontvangt Verwerker rechtstreeks een verzoek van een betrokkene dat de Klantdata betreft, dan verwijst Verwerker de betrokkene naar de Klant en informeert Verwerker de Klant, tenzij dat wettelijk niet is toegestaan. Verwerker reageert op verzoeken van de Klant binnen een zodanige termijn dat de Klant de wettelijke termijn van één maand kan halen.

9.4 Aanvullende, handmatige bijstand die de zelfservicefunctionaliteit van de Dienst te boven gaat, verleent Verwerker op verzoek (via info@vastly.software) tegen het alsdan geldende **uurtarief** van Verwerker; Verwerker geeft de Klant vooraf een indicatie van de verwachte omvang.

Artikel 10 — Meldplicht datalekken

10.1 Verwerker informeert de Klant **onverwijld, doch uiterlijk binnen 48 uur** nadat Verwerker een inbreuk in verband met persoonsgegevens die Klantdata (mogelijk) raakt heeft ontdekt, via het bij Verwerker bekende contactadres van de Klant.

10.2 De melding bevat, voor zover op dat moment bekend: de aard van de inbreuk, de (categorieën) betrokkenen en persoonsgegevensregisters in kwestie en een schatting van de aantallen, de waarschijnlijke gevolgen en de genomen of voorgestelde maatregelen. Informatie die nog niet beschikbaar is wordt in stappen nageleverd.

10.3 De beoordeling of melding aan de Autoriteit Persoonsgegevens en/of de betrokkenen vereist is, en het doen van die melding, is aan de Klant als verwerkingsverantwoordelijke. Verwerker ondersteunt daarbij met de beschikbare informatie, waaronder reconstructie op basis van het audit-/logspoor (Bijlage 2).

10.4 Verwerker documenteert inbreuken en de respons daarop en meldt een inbreuk niet zelfstandig aan betrokkenen of media, behoudens een wettelijke plicht daartoe.

Artikel 11 — Bijstand bij beveiliging, DPIA en voorafgaande raadpleging

11.1 Rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie verleent Verwerker de Klant bijstand bij het nakomen van de verplichtingen uit art. 32 t/m 36 AVG (beveiliging, melding van inbreuken, gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging), onder meer door het verstrekken van de in Bijlage 2 beschreven maatregelen en relevante informatie over de verwerking. Artikel 9.4 over kosten is van overeenkomstige toepassing.

Artikel 12 — Audit- en inzagerecht

12.1 Verwerker stelt de Klant alle informatie ter beschikking die nodig is om de nakoming van de in artikel 28 AVG neergelegde verplichtingen aan te tonen, en maakt audits — waaronder inspecties — door de Klant of een door de Klant gemachtigde (niet-concurrerende) auditor mogelijk en draagt eraan bij.

12.2 De volgorde is: (i) beantwoording op basis van beschikbare documentatie en het bestaande audit-exportspoor (WORM-export, Bijlage 2); (ii) pas als dat aantoonbaar tekortschiet een audit op locatie of systeemniveau, **maximaal éénmaal per twaalf maanden**, schriftelijk aangekondigd met een termijn van ten minste **30 dagen**, tijdens kantooruren, zonder onnodige verstoring van de dienstverlening en onder geheimhouding; gegevens van andere klanten blijven daarbij buiten bereik. De kosten van een audit draagt de Klant, tenzij uit de audit een **toerekenbare tekortkoming** van Verwerker blijkt.

Artikel 13 — Aansprakelijkheid

13.1 De totale aansprakelijkheid van Verwerker jegens de Klant uit hoofde van of in verband met deze VWO is per gebeurtenis (waarbij een reeks samenhangende gebeurtenissen als één gebeurtenis geldt) en per contractjaar beperkt tot het bedrag van de door de Klant aan Verwerker betaalde vergoedingen over de **twaalf maanden** voorafgaand aan de gebeurtenis waaruit de schade voortvloeit.

13.2 Aansprakelijkheid van Verwerker voor **indirecte schade** — waaronder gevolgschade, gederfde winst, gemiste besparingen, schade door bedrijfsstagnatie en reputatieschade — is uitgesloten.

13.3 De beperkingen van 13.1 en 13.2 gelden niet in geval van **opzet of bewuste roekeloosheid** van Verwerker of diens bedrijfsleiding, noch voor zover aansprakelijkheid op grond van dwingend recht niet kan worden beperkt of uitgesloten.

13.4 In de onderlinge verhouding tussen Partijen draagt, conform art. 82 AVG, ieder van Partijen de schade en de opgelegde administratieve boetes voor zover die zijn veroorzaakt door zijn eigen niet-nakoming van de op hem rustende verplichtingen uit de AVG of deze VWO; de partij die op grond van art. 82 lid 4 AVG meer heeft vergoed dan het deel dat hem aangaat, heeft verhaal op de andere partij overeenkomstig art. 82 lid 5 AVG.

Artikel 14 — Duur, einde, teruggave en verwijdering

14.1 Deze VWO treedt in werking bij het aangaan van de Hoofdovereenkomst en geldt zolang Verwerker Klantdata verwerkt. De Hoofdovereenkomst is opzegbaar op elke dag; de Hoofdovereenkomst eindigt **30 dagen na de dag van opzegging**, ongeacht de kalendermaand. De laatste abonnementsperiode wordt naar rato in rekening gebracht; reeds betaalde perioden worden niet gerestitueerd.

14.2 **Teruggave door zelfservice.** De Klant kan zijn gegevens gedurende de gehele looptijd én gedurende de Read-only-naperiode zelf downloaden via de Zelfservice-export. Vanaf de einddatum van de Hoofdovereenkomst geldt een **Read-only-naperiode van 30 dagen**: gebruikers van de Klant behouden leestoegang binnen de eigen omgeving en de Zelfservice-export blijft beschikbaar; wijzigingen zijn niet meer mogelijk.

14.3 **Verwijdering ná de naperiode.** Na afloop van de Read-only-naperiode beëindigt Verwerker de toegang en verwijdert Verwerker de Klantdata definitief. "Verwijderd" betekent: de productiedatabase en de documentopslag zijn geleegd per het verwijdermoment, en back-ups/herstelpunten lopen binnen **7 dagen** na het verwijdermoment uit; het langetermijnarchief van Verwerker bevat per ontwerp geen Klantdata. De verwijdering is een mens-bevestigde, onherroepelijke handeling die in het auditspoor wordt vastgelegd (aantallen per tabel/opslag, nooit de oude waarden).

14.4 **Overgang van de bewaarplicht.** Verwerker neemt geen (fiscale of andere wettelijke) bewaarplicht over de Klantdata op zich. Vanaf het verwijdermoment ligt de wettelijke bewaarplicht over de administratie volledig bij de Klant; de Klant is er zelf voor verantwoordelijk zijn gegevens vóór het einde van de Read-only-naperiode te downloaden. Dit regime wordt bij opzegging bovendien uitdrukkelijk aan de Klant voorgelegd en door de Klant bevestigd (verplichte bevestigingsverklaring in de opzegflow, inhoudelijk gelijk aan dit artikel).

14.5 **Drie uitzonderingen** op de verwijdering:

a. de facturen die Verwerker zélf aan de Klant heeft gestuurd (abonnementsfacturen): eigen administratie van Verwerker, bewaard onder de eigen fiscale bewaarplicht (7 jaar); en

b. het technische audit-/bewijsspoor: dit is bij ontwerp onveranderbaar (append-only) en kan niet worden verwijderd; het wordt bij de verwijdering **gepseudonimiseerd** zodat het niet langer tot de Klant of betrokkenen herleidbaar is; en

c. de onderdrukkingslijst van het verzendkanaal: e-mailadressen die als onbestelbaar zijn gemeld of waarvan de ontvanger geen e-mail meer wil, blijven uitsluitend als **gepseudonimiseerde** waarde (hash met een vaste sleutel, niet terug te rekenen) bewaard, zodat Verwerker ook na het einde van de Hoofdovereenkomst niet opnieuw naar die adressen verzendt (grondslag: gerechtvaardigd belang van Verwerker en van de betrokkene).

Artikel 15 — Slotbepalingen

15.1 Wijzigingen van deze VWO gelden alleen indien schriftelijk overeengekomen, met uitzondering van de actualisaties bedoeld in artikel 6.2 (Bijlage 2) en de procedure van artikel 7.3 (Bijlage 1).

15.2 Indien een bepaling van deze VWO nietig of vernietigbaar blijkt, blijft het overige onverminderd van kracht en vervangen Partijen de betreffende bepaling door een geldige bepaling die de strekking zo dicht mogelijk benadert.

15.3 Op deze VWO is **Nederlands recht** van toepassing. Geschillen worden voorgelegd aan de bevoegde rechter van de **rechtbank Gelderland, locatie Arnhem**.

Ondertekening

	Verwerkingsverantwoordelijke	**Verwerker**
Naam	[naam]	[naam], PDL Powerhouse B.V. (Vastly)
Functie	[functie]	[functie]
Datum	[datum]	[datum]
Handtekening		

Bijlage 1 — Subverwerkers (stand 2026-09-24, ongewijzigd in v1.2)

Subverwerker	**Rol / verwerking**	**Locatie verwerking en doorgiftemechanisme**
Google Cloud EMEA Limited (onder de actuele Google Cloud Data Processing Addendum)	Hosting van applicatie en database (Cloud Run, Cloud SQL) en documentopslag (Cloud Storage), incl. back-ups	Regio europe-west4 (Nederland); verwerking binnen de EU. Doorgifte (voor zover aan de orde): DPF-certificering, SCC's als terugval (art. 8.2)

Subverwerker	Rol / verwerking	Locatie verwerking en doorgiftemechanisme
Google Cloud EMEA Limited — Google Workspace (onder de actuele Google Cloud Data Processing Addendum)	Uitsluitend de eigen mailbox info@vastly.software van Verwerker (contact- en supportverkeer). Facturen/herinneringen aan huurders verstuurt de Klant vanuit de eigen gekoppelde mailbox — die koppeling is geen subverwerking door Google Workspace	EU-verwerkingsafspraken conform de Google-DPA. Doorgifte (voor zover aan de orde): DPF-certificering, SCC's als terugval (art. 8.2)
Amazon Web Services EMEA SARL — Amazon SES (v1.1)	Verzending van e-mail vanuit de Dienst: systeemberichten van Verwerker (uitnodigingen, inlogcodes, servicemeldingen) en, alleen als de Klant daarvoor kiest, berichten aan huurders namens de Klant (huurnota's, herinneringen, aanzeggingen); verwerkt e-mailadres, onderwerp, berichttekst en bijlagen tijdens transport en bezorgstatus	Regio eu-west-1 (Ierland); verwerking binnen de EU onder de AWS-DPA. Doorgifte (voor zover aan de orde): DPF-certificering, SCC's als terugval (art. 8.2)
Online Payment Platform B.V. (v1.1)	Verwerking van huurbetalingen die via de Dienst worden gestart (iDEAL-betaallink per huurnota): betaalgegevens en betaalstatus van huurders binnen het sub-merchant-account van de Klant. Voor de KYC van de Klant en de uitbetaling is OPP zelfstandig verwerkingsverantwoordelijke (art. 7.4 sub b)	Nederland (EU); vergunninghoudende betaalinstelling (DNB)
Yousign SAS — via contractpartij **Youtrust** (v1.1: contractpartij toegevoegd)	Elektronische ondertekening van huurovereenkomsten met een geavanceerde elektronische handtekening (huurders) en van overige documenten (incl. identificatiegegevens ondertekenaars, bewijsdossier)	EU (Frankrijk)
Expo (Expo.dev)	Technische bezorging van push-notificaties naar de mobiele app (bezorg-tokens en berichtkoppen) en het uitrollen van app-updates	VS. Doorgifte: DPF-certificering, SCC's als terugval (art. 8.2)
Anthropic (v1.1: standaard aan sinds 13-09-2026)	AI-functies "notarisstukken voorlezen" en "kamers uit de plattegrond voorlezen": verwerking van het door de Klant geüploade document door de Claude-API onder verwerkersafspraken (DPA) om waarden voor te stellen die de Klant zelf bevestigt; geen gebruik voor modeltraining, geen bewaring na verwerking. De Klant kan de functie per verhuurder via Verwerker laten uitzetten	Doorgifte (voor zover buiten de EER): geldig mechanisme conform art. 8.2 (DPA met SCC's); passage conform privacyverklaring §5

Subverwerker	Rol / verwerking	Locatie verwerking en doorgiftemechanisme
Company.info (v1.1)	Bevraging van het Handelsregister bij registratie en bij de controle van tekenbevoegdheid van vertegenwoordigers van de Klant: bedrijfsnaam of KvK-nummer van de Klant, terugontvangen openbare registergegevens (inschrijving, functionarissen). Geen huurdergegevens	Nederland (EU)

Geen subverwerker, wel relevant (ontvangers, art. 7.4): betaaldienstverlener **Mollie B.V.** (betaallinks via het account van de Klant; eigen verkopen van Verwerker), **Online Payment Platform B.V.** voor de KYC en uitbetaling van de Klant, en een toekomstige bankkoppeling via een vergunninghoudende rekeninginformatiedienstverlener (AISP, PSD2) zijn zelfstandig verwerkingsverantwoordelijke. De actuele subverwerkersinformatie is opvraagbaar via info@vastly.software.

Bijlage 2 — Technische en organisatorische maatregelen (stand 2026-08-22)

Hosting en versleuteling

- Alle verwerking en opslag in Google Cloud-regio europe-west4 (Nederland); verwerking binnen de EU.
- Versleuteling in transit: alle verbindingen via TLS.
- Versleuteling at rest met door Verwerker beheerde sleutels (**CMEK**) op zowel de productiedatabase als de documentopslag (Cloud KMS, keyring in europe-west4, automatische jaarlijkse sleutelrotatie).
- Database uitsluitend bereikbaar via privé-IP (geen publiek endpoint); koppelingen via least-privilege-serviceaccounts.
- Geheimen (API-sleutels, tokens) uitsluitend in Secret Manager; nooit in code, logs of configuratiebestanden.

Toegang en authenticatie

- Inloggen met **passkeys** als eerste authenticatielijn; wachtwoord met tweestapsverificatie (TOTP) als terugval-/herstelroute. Sessies verlopen automatisch; refresh-tokens zijn apparaatsgebonden.
- Logische scheiding per klant/eigenaar, afgedwongen in de autorisatielaag van de applicatie: iedere gebruiker ziet uitsluitend de gegevens binnen de eigen organisatie-scope (rol- en scopemodel, gedocumenteerde rechtenmatrix). Beheerstoegang (superadmin-console) is strikt gescheiden van klantomgevingen.
- Rol- en scope-mutaties zijn voorbehouden aan beheerders; niemand kan de eigen rol wijzigen.

Controleerbaarheid en integriteit

- Append-only audit-logboek (audit_event) van wijzigingen en beheerhandelingen, met WORM-export als bewijsvorm; het auditspoor is bij ontwerp onveranderbaar.
- Mens-in-de-lus voor uitgaande acties en destructieve handelingen (verzending, verwijdering): geen autonome onomkeerbare acties.

Beschikbaarheid en herstel

- Automatische back-ups en point-in-time-recovery van de productiedatabase (retentievenster 7 dagen; dit venster is tevens de uitloopgrens van artikel 14.3).
- Gescheiden test- en productieomgevingen; geautomatiseerde tests op de reken- en verwerkingslogica.

Organisatorisch

- Vertrouwelijkheidsverplichting voor personen met toegang (artikel 5).
- Beveiligingsincidentproces met documentatieplicht (artikel 10.4).

Deze bijlage beschrijft uitsluitend feitelijk getroffen maatregelen; de passendheid ervan is vastgesteld in artikel 6.3.