Verwerkersovereenkomst Colli Control

Verwerkersovereenkomst op grond van artikel 28 AVG: de verwerking van persoonsgegevens door Colli Control voor de klant, met subverwerkers en beveiligingsmaatregelen.

Versie 1.1 · geldig vanaf 9 november 2026 ·

Partijen

`Klant` , zoals genoemd in de Abonnementsovereenkomst, hierna: Klant of verwerkingsverantwoordelijke;

`Alec van der Doef` , handelend onder de naam Colli Control, ingeschreven bij de Kamer van Koophandel onder nummer 42154037, gevestigd te Hoek van Holland, hierna: Leverancier of verwerker.

Artikel 1 Definities

1.1 Begrippen uit de Algemene Verordening Gegevensbescherming (AVG), zoals persoonsgegevens, verwerking, betrokkene, verwerkingsverantwoordelijke, verwerker en inbreuk in verband met persoonsgegevens, hebben de betekenis die de AVG eraan geeft.

1.2 Begrippen met een hoofdletter die hier niet zijn gedefinieerd, hebben de betekenis uit de Algemene Voorwaarden Colli Control (AV).

1.3 Subverwerker: een derde die Leverancier inschakelt en die bij de uitvoering van de Overeenkomst persoonsgegevens verwerkt voor Klant.

1.4 Inbreuk: een inbreuk in verband met persoonsgegevens als bedoeld in artikel 4 onder 12 AVG, die persoonsgegevens raakt die Leverancier voor Klant verwerkt.

Artikel 2 Onderwerp en rolverdeling

2.1 Deze verwerkersovereenkomst maakt deel uit van de Overeenkomst. Zij geldt voor alle persoonsgegevens die Leverancier bij de uitvoering van de Overeenkomst voor Klant verwerkt.

2.2 Klant is verwerkingsverantwoordelijke en Leverancier is verwerker. De aard en de doelen van de verwerking, de soorten persoonsgegevens en de categorieën betrokkenen staan in bijlage 1.

2.3 Klant staat ervoor in dat de verwerking rechtmatig is, dat hij daarvoor een grondslag heeft en dat hij de betrokkenen informeert. Klant bepaalt zelf welke persoonsgegevens hij in de Dienst invoert.

2.4 Voor verwerkingen die Leverancier voor eigen doeleinden uitvoert, zoals accountbeheer, facturatie, beveiliging van de Dienst en contact met Klant, is Leverancier zelf verwerkingsverantwoordelijke. Daarvoor geldt zijn privacyverklaring en niet deze overeenkomst.

Artikel 3 Instructies

3.1 Leverancier verwerkt persoonsgegevens uitsluitend op basis van de Schriftelijke instructies van Klant, ook bij doorgifte buiten de EER. Die instructies bestaan uit de Overeenkomst, de configuratie die Klant in de Dienst aanbrengt en nadere Schriftelijke instructies.

3.2 Leverancier mag afwijken als een wettelijke verplichting hem dat oplegt. Hij informeert Klant daar vooraf over, tenzij de wet dat verbiedt.

3.3 Leverancier meldt direct als een instructie naar zijn oordeel in strijd is met de AVG of andere regels voor gegevensbescherming.

3.4 Klant geeft Leverancier de instructie om gegevens over het gebruik en de prestaties van de Dienst te anonimiseren en geaggregeerd te gebruiken om de Dienst te verbeteren, zoals bepaald in artikel 12.2 AV. Voor andere eigen doeleinden verwerkt Leverancier de persoonsgegevens niet.

3.5 Vergt een nadere instructie werkzaamheden buiten de Dienst, dan mag Leverancier die als Maatwerk in rekening brengen. Dat geldt niet voor instructies die Leverancier nodig heeft om zelf aan de AVG te voldoen.

Artikel 4 Geheimhouding

4.1 Leverancier houdt de persoonsgegevens geheim. Iedereen die namens Leverancier toegang heeft tot persoonsgegevens, is aan geheimhouding gebonden via een arbeids- of opdrachtovereenkomst of een aparte geheimhoudingsverklaring.

4.2 Leverancier geeft alleen toegang aan personen die de gegevens nodig hebben voor de uitvoering van de Overeenkomst, en alleen voor zover dat nodig is.

Artikel 5 Beveiliging

5.1 Leverancier neemt passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen, zoals bedoeld in artikel 32 AVG. De maatregelen staan in bijlage 3.

5.2 Leverancier evalueert de maatregelen periodiek en ten minste eenmaal per jaar. Hij mag ze aanpassen aan de stand van de techniek, zolang het beveiligingsniveau niet daalt.

5.3 Klant heeft de maatregelen in bijlage 3 beoordeeld en vindt ze passend voor de verwerking uit bijlage 1. Klant meldt het Schriftelijk als hij persoonsgegevens met een hoger risico wil verwerken dan in bijlage 1 staat.

5.4 Klant is verantwoordelijk voor de beveiliging aan zijn kant, zoals het beheer van Accounts, rechten, sharelinks en Externe Gebruikers (artikel 5 en 6 AV).

Artikel 6 Subverwerkers

6.1 Klant geeft Leverancier algemene Schriftelijke toestemming om Subverwerkers in te schakelen. De huidige Subverwerkers staan in bijlage 2.

6.2 Leverancier meldt een nieuwe of vervangende Subverwerker ten minste 30 dagen vooraf Schriftelijk. Klant kan binnen 14 dagen na de melding op redelijke gronden bezwaar maken.

6.3 Bij een bezwaar zoeken partijen samen naar een oplossing. Lukt dat niet binnen 30 dagen, dan mag Klant de Overeenkomst opzeggen tegen de datum waarop de Subverwerker wordt ingezet, zonder kosten. Leverancier betaalt vooruitbetaalde vergoedingen dan naar rato terug.

6.4 Moet een Subverwerker dringend worden vervangen om de beveiliging of continuïteit van de Dienst te waarborgen, dan mag Leverancier dat direct doen. Hij meldt het Klant dan zo snel mogelijk, en lid 3 geldt vanaf die melding.

6.5 Leverancier legt elke Subverwerker ten minste gelijkwaardige verplichtingen op als in deze overeenkomst, in het bijzonder voor beveiliging. Bij grote infrastructuurleveranciers gebeurt dat via hun standaard-verwerkersovereenkomst.

6.6 Leverancier blijft tegenover Klant volledig verantwoordelijk voor de nakoming door zijn Subverwerkers (artikel 28 lid 4 AVG), binnen de grenzen van artikel 17 AV.

Artikel 7 Doorgifte buiten de EER

7.1 Leverancier slaat persoonsgegevens op binnen de Europese Economische Ruimte (EER). Uitzondering zijn de gegevens die nodig zijn om e-mails vanuit de Dienst te versturen, en de toegang tot gebruiksgegevens voor productanalyse, zoals vermeld in bijlage 2.

7.2 Doorgifte naar een land buiten de EER, ook in de vorm van toegang op afstand, vindt alleen plaats als aan hoofdstuk V AVG is voldaan. Dat kan op grond van een adequaatheidsbesluit, waaronder het EU-VS Data Privacy Framework voor gecertificeerde partijen, of op grond van de standaardcontractbepalingen van de Europese Commissie met zo nodig aanvullende maatregelen.

7.3 Bijlage 2 vermeldt per Subverwerker of er doorgifte plaatsvindt en op welke grond. Met deze overeenkomst geeft Klant de instructie voor die doorgiften.

7.4 Ontvangt Leverancier of een Subverwerker een verzoek van een overheidsinstantie buiten de EER om persoonsgegevens te verstrekken, dan informeert Leverancier Klant daarover voor zover dat is toegestaan. Leverancier verstrekt alleen gegevens als hij daartoe wettelijk verplicht is, en betwist een verzoek dat hij onrechtmatig acht.

Artikel 8 Inbreuken in verband met persoonsgegevens

8.1 Leverancier meldt een Inbreuk zonder onredelijke vertraging aan Klant, en uiterlijk 48 uur nadat hij de Inbreuk heeft ontdekt. Zo kan Klant zelf binnen 72 uur melden aan de Autoriteit Persoonsgegevens (artikel 33 AVG).

8.2 De melding bevat, voor zover bekend:

- de aard van de Inbreuk;
- de categorieën en het geschatte aantal betrokkenen en gegevensrecords;
- de waarschijnlijke gevolgen;
- de maatregelen die Leverancier heeft genomen of voorstelt;
- een contactpersoon voor verdere informatie.

8.3 Is niet alle informatie direct beschikbaar, dan meldt Leverancier gefaseerd. Hij houdt Klant op de hoogte van de ontwikkelingen.

8.4 Klant beslist of de Inbreuk wordt gemeld aan de toezichthouder en aan betrokkenen. Leverancier meldt niet zelf, tenzij de wet hem daartoe verplicht.

8.5 Leverancier neemt direct redelijke maatregelen om de Inbreuk te beperken en herhaling te voorkomen. Hij houdt een register bij van alle Inbreuken.

8.6 Elke partij draagt haar eigen kosten van een melding. Is de Inbreuk aan Leverancier toe te rekenen, dan geldt artikel 11.

Artikel 9 Rechten van betrokkenen en DPIA

9.1 De Dienst biedt Klant functies om persoonsgegevens zelf in te zien, te corrigeren, te verwijderen en te exporteren. Waar die functies niet volstaan, helpt Leverancier Klant met passende maatregelen om verzoeken van betrokkenen te beantwoorden.

9.2 Ontvangt Leverancier een verzoek rechtstreeks van een betrokkene, dan stuurt hij het direct door naar Klant. Leverancier beantwoordt het verzoek niet zelf, tenzij Klant hem dat opdraagt.

9.3 Leverancier werkt redelijkerwijs mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en aan een eventuele voorafgaande raadpleging van de toezichthouder (artikelen 35 en 36 AVG).

9.4 Voor medewerking die meer dan 2 uur per kalenderjaar kost, mag Leverancier het geldende uurtarief rekenen. Dat geldt niet als de medewerking nodig is door een tekortkoming van Leverancier.

Artikel 10 Informatie en audit

10.1 Leverancier stelt Klant alle informatie ter beschikking die nodig is om aan te tonen dat hij deze overeenkomst en artikel 28 AVG nakomt. Dat gebeurt in de eerste plaats met documentatie, zoals bijlage 3, de beveiligingsvragenlijst uit artikel 10.3 AV en rapporten of certificaten van Subverwerkers.

10.2 Volstaat die documentatie aantoonbaar niet, dan mag Klant een audit laten uitvoeren. Dat kan hoogstens eenmaal per jaar, na een aankondiging van ten minste 30 dagen, door een onafhankelijke deskundige met een geheimhoudingsplicht. De audit mag de Dienst niet verstoren.

10.3 Klant draagt de kosten van de audit. Blijkt uit de audit dat Leverancier deze overeenkomst op wezenlijke punten niet nakomt, dan draagt Leverancier zijn eigen kosten en herstelt hij de tekortkomingen binnen een redelijke termijn.

10.4 Een onderzoek door een toezichthouder is altijd mogelijk, los van de beperkingen in dit artikel.

Artikel 11 Aansprakelijkheid

11.1 Voor de aansprakelijkheid van partijen onder deze overeenkomst geldt artikel 17 AV.

11.2 Elke partij draagt zelf een boete die de toezichthouder aan haar oplegt.

11.3 Wordt een partij door een betrokkene aangesproken op grond van artikel 82 AVG, dan draagt de andere partij in de onderlinge verhouding het deel van de schade dat aan haar is toe te rekenen, binnen de grenzen van artikel 17 AV.

11.4 Klant vrijwaart Leverancier voor aanspraken die voortvloeien uit een instructie van Klant die in strijd is met de AVG.

Artikel 12 Duur, teruggave en verwijdering

12.1 Deze overeenkomst geldt zolang Leverancier persoonsgegevens voor Klant verwerkt. Opzegging los van de Overeenkomst is niet mogelijk.

12.2 Na het einde van de Overeenkomst stelt Leverancier de persoonsgegevens beschikbaar voor export en verwijdert hij ze daarna, volgens artikel 16 AV. Klant bepaalt binnen de ophaalperiode of hij de gegevens wil laten exporteren.

12.3 Leverancier verwijdert ook alle kopieën, tenzij het Unierecht of Nederlands recht bewaring verplicht. Uit back-ups verdwijnen de gegevens zodra de back-upcyclus uit artikel 16.6 AV is verstreken. Tot dat moment blijven de back-ups onder deze overeenkomst vallen.

12.4 Leverancier bevestigt de verwijdering Schriftelijk.

12.5 Bepalingen die naar hun aard doorlopen, zoals geheimhouding en aansprakelijkheid, blijven na het einde van deze overeenkomst gelden.

Artikel 13 Slotbepalingen

13.1 Klant aanvaardt deze overeenkomst door de Abonnementsovereenkomst te ondertekenen, waarin naar deze overeenkomst wordt verwezen. Een elektronische ondertekening volstaat (artikel 28 lid 9 AVG).

13.2 Bij strijdigheid gaat deze overeenkomst voor de verwerking van persoonsgegevens voor de AV. Voor aansprakelijkheid gaat artikel 17 AV voor.

13.3 Leverancier mag bijlage 2 en bijlage 3 bijwerken volgens artikel 5.2 en artikel 6. Andere wijzigingen vergen Schriftelijke instemming van beide partijen.

13.4 Verandert de wet zodanig dat deze overeenkomst moet worden aangepast, dan werken partijen daar in redelijkheid aan mee.

13.5 Op deze overeenkomst is Nederlands recht van toepassing. Geschillen worden beslecht volgens artikel 22 AV.

Bijlage 1 — Specificatie van de verwerking

`Doelen.` Leverancier verwerkt de persoonsgegevens om de Dienst te leveren: orderbeheer, expeditie- en transportplanning, documentatie, samenwerking met ketenpartners via portals, gebruikersbeheer, beveiliging en auditlogging, support en foutopsporing, en productanalyse om de Dienst te verbeteren.

`Aard van de verwerking.` Opslaan, ordenen, raadplegen, synchroniseren met het ERP-systeem van Klant, verwerken in Output en documenten, delen met Externe Gebruikers volgens de instellingen van Klant, back-uppen, exporteren en verwijderen. De verwerking loopt doorlopend zolang de Overeenkomst duurt.

Categorie betrokkenen	Soorten persoonsgegevens
Gebruikers bij Klant (planners, expeditie, sales, beheerders)	Naam, zakelijk e-mailadres, functie en rol, inloggegevens, MFA-gegevens, IP-adres, sessie- en auditloggegevens
Externe Gebruikers (medewerkers van afnemers, transporteurs en andere ketenpartners)	Naam, zakelijk e-mailadres, organisatie, rol, inloggegevens, IP-adres, sessie- en auditloggegevens
Contactpersonen bij afnemers en transporteurs	Naam, zakelijke contactgegevens en organisatie, zoals vastgelegd in orders en transporten
Overige personen	Persoonsgegevens die Klant zelf opneemt in vrije tekstvelden, aangepaste velden, mededelingen of geüploade documenten

Geen bijzondere gegevens. De Dienst is niet bedoeld voor bijzondere persoonsgegevens, strafrechtelijke gegevens of het burgerservicenummer (artikelen 9 en 10 AVG). Klant voert die niet in de Dienst in.

Bewaartermijnen.

Gegevens	Bewaartermijn
Klantdata	Looptijd van de Overeenkomst, daarna verwijdering volgens artikel 16 AV
Auditlog	90 dagen; met de module Security en compliance tot 7 jaar, zoals Klant instelt
Back-ups	Tot het einde van de back-upcyclus uit artikel 16.6 AV
Foutmeldingen in Sentry	Volgens de bewaartermijn van het Sentry-abonnement; foutmeldingen bevatten zo min mogelijk persoonsgegevens
Productanalyse in PostHog	1 jaar; schermopnames 30 dagen. Geen namen, e-mailadressen, IP-adressen of inhoud van orders en documenten

Bijlage 2 — Subverwerkers

Klantdata staat in de EER. Doorgifte buiten de EER is beperkt tot toegang voor support en beheer, foutmeldingen, productanalyse en het versturen van e-mail, op de grondslagen hieronder. Stand: 9 november 2026.

Subverwerker	Dienst	Locatie gegevens	Doorgifte buiten de EER en grondslag
Supabase Pte. Ltd. (https://supabase.com/legal/customer-resources/data-processing-addendum), Singapore	Authenticatie (inloggen)	AWS eu-north-1, Stockholm (Zweden)	Toegang op afstand door de Supabase-groep voor support en beheer. Grondslag: EU-standaardcontractbepalingen in de DPA van Supabase
Microsoft Ireland Operations Ltd. (https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn), Ierland	Hosting van de webapplicatie en het beheerportaal (Azure Static Web Apps); de API, achtergrondtaken, realtime-updates en ERP-synchronisatie (Azure Container Apps); de database (Azure Database for PostgreSQL); opslag van documenten, bestanden en back-ups, met een malwarescan bij het uploaden (Azure Blob Storage met Microsoft Defender for Storage)	Azure-regio's North Europe (Ierland) en West Europe (Nederland), binnen de EU Data Boundary	Alleen in de beperkte uitzonderingen van de EU Data Boundary, zoals support. Grondslag: Data Privacy Framework en EU-standaardcontractbepalingen in de DPA van Microsoft
Functional Software, Inc. (Sentry) (https://sentry.io/legal/dpa/), Verenigde Staten	Foutmonitoring van de webapplicatie, het beheerportaal en de API. IP-adressen worden niet opgeslagen	EU-regio, Frankfurt (Duitsland)	Toegang door een Amerikaanse entiteit. Grondslag: EU-VS Data Privacy Framework, met EU-standaardcontractbepalingen als terugval
PostHog Inc. (https://posthog.com/dpa), Verenigde Staten	Productanalyse van de webapplicatie: een willekeurige gebruikers-id, organisatie-id, rol en accounttype, bezochte schermen als patroon en een	EU-regio, Frankfurt (Duitsland); subverwerkers van PostHog volgens posthog.com/subprocessors (https://posthog.com/subprocessors)	Toegang door een Amerikaanse entiteit en haar subverwerkers. Grondslag: EU-VS Data Privacy Framework, met EU-standaardcontractbepalingen (module 2) in de DPA van PostHog

Subverwerker	Dienst	Locatie gegevens	Doorgifte buiten de EER en grondslag
	beperkte set gebeurtenissen, eventueel volledig gemaskeerde schermopnames. Geen namen, e-mailadressen of IP-adressen; Klant kan productanalyse uitzetten		
Plus Five Five, Inc. (Resend) (https://resend.com/legal/dpa), Verenigde Staten	Transactionele e-mail, zoals uitnodigingen, wachtwoordherstel en notificaties	Verzending vanuit de EU-regio (Ierland); accountgegevens, metadata en logs in de Verenigde Staten	Ja: e-mailadressen, namen en inhoud van e-mails worden in de VS opgeslagen. Grondslag: EU-VS Data Privacy Framework en EU-standaardcontractbepalingen in de DPA van Resend

Voor uptime-monitoring gebruikt Leverancier Better Stack. Die dienst controleert alleen de bereikbaarheid van publieke adressen, verwerkt geen persoonsgegevens voor Klant en is daarom geen Subverwerker.

Bijlage 3 — Technische en organisatorische maatregelen

Deze maatregelen gelden als toezegging aan Klant.

Onderwerp	Maatregel
Scheiding tussen klanten	Elke klant is een aparte tenant. Row Level Security in de database dwingt die scheiding af op databaseniveau, los van de applicatielogica.
Toegang in de Dienst	Rollen en rechten per Gebruiker en per Bedrijf. Externe Gebruikers zien alleen de orders en transporten die aan hen zijn toegewezen. MFA-afdwinging, IP-restricties en sessiebeleid zijn beschikbaar via de module Security en compliance.
Beheertoegang Leverancier	Toegang tot productiesystemen (Supabase, Azure, GitHub) alleen voor Leverancier, met MFA en persoonlijke accounts. Klantdata wordt alleen ingezien als dat nodig is voor support of incidentafhandeling.
Versleuteling	Verkeer is versleuteld met TLS. Gegevens in de database en bestandsopslag zijn versleuteld opgeslagen door de hostingleveranciers.
Monitoring	Uptime-monitoring met alarmering (Better Stack) en foutmonitoring (Sentry, EU-regio). Foutmeldingen worden zo ingesteld dat ze zo min mogelijk persoonsgegevens bevatten.
Auditlog	Handelingen in de Dienst worden gelogd met gebruiker en tijdstip. De bewaartermijn staat in bijlage 1.
Wijzigingsbeheer	Broncode in versiebeheer. Wijzigingen lopen via pull requests met geautomatiseerde codereview voordat ze naar productie gaan. Test en productie zijn gescheiden, en productiedata wordt niet voor testen gebruikt.
Incidenten en datalekken	Vaste procedure voor Inbreuken, met melding aan Klant binnen 48 uur (artikel 8) en een register van Inbreuken.
Organisatie	Geheimhouding voor iedereen met toegang (artikel 4), een verwerkingsregister (artikel 30 lid 2 AVG), beoordeling van Subverwerkers voordat ze worden ingezet, en een jaarlijkse evaluatie van deze maatregelen.

Versiegeschiedenis

Versie 1.1 — geldig vanaf 9 november 2026

Versie 1.0 — geldig vanaf 23 september 2026