MODEL-DPA · ARTIKEL 28 AVG

Verwerkersovereenkomst

Data Processing Agreement

Deze overeenkomst legt vast hoe IMDigital, handelend onder de naam Infaris, persoonsgegevens verwerkt in opdracht van een zakelijke klant. Zij is opgesteld voor toepassing van artikel 28 AVG en hoort bij de hoofdovereenkomst waaronder de Infaris-diensten worden afgenomen.

VERWERKER	REGISTRATIE	VESTIGING	VERSIE
IMDigital, h.o.d.n. Infaris	KVK 95452354	Grebbeweg 19B, 3902 HG Veenendaal	1.1 · 12 september 2026

In te vullen vóór ondertekening

VERWERKINGSVERANTWOORDELIJKE	[VOLLEDIGE NAAM KLANT]
VESTIGINGSADRES EN KVK	[ADRES] · [KVK-NUMMER]
INGANGSDATUM	[DATUM]
HOOFDOVEREENKOMST	[NAAM ABONNEMENT, OFFERTE OF DIENSTENOVEREENKOMST]
AFGENOMEN DIENSTEN	[GUARD / FILES / CALENDAR / PRESENT / SUPPORT / OVERIG]

Status: model voor contractuele afstemming en ondertekening. Laat de definitieve versie, met name de klantspecifieke instructies, bewaartermijnen en ingeschakelde subverwerkers, vóór gebruik juridisch beoordelen.

DEEL 1

Partijen en overwegingen

Deze verwerkersovereenkomst (de "DPA") wordt gesloten tussen de op het voorblad genoemde klant (de "Verwerkingsverantwoordelijke") en IMDigital, handelend onder de naam Infaris (de "Verwerker"). Verwerkingsverantwoordelijke en Verwerker worden gezamenlijk aangeduid als "Partijen".

Verwerkingsverantwoordelijke bepaalt de doeleinden en middelen van de verwerking van Persoonsgegevens. Verwerker verwerkt Persoonsgegevens uitsluitend ten behoeve van de levering van de Infaris-diensten en overeenkomstig gedocumenteerde instructies van Verwerkingsverantwoordelijke. Partijen willen hun afspraken vastleggen overeenkomstig de AVG, in het bijzonder artikel 28.

ARTIKEL 01 Definities en rangorde

Begrippen met een hoofdletter hebben de betekenis die de AVG daaraan geeft. Onder "AVG" wordt verstaan Verordening (EU) 2016/679. "Diensten" zijn de Infaris-diensten die Verwerkingsverantwoordelijke op grond van de Hoofdovereenkomst afneemt. "Persoonsgegevens" zijn de persoonsgegevens die Verwerker in opdracht van Verwerkingsverantwoordelijke verwerkt. "Inbreuk in verband met persoonsgegevens" wordt hierna aangeduid als "Datalek".

Deze DPA is onderdeel van de Hoofdovereenkomst. Bij strijdigheid over de verwerking van Persoonsgegevens gaat deze DPA voor. De Hoofdovereenkomst blijft voor het overige van kracht. De bijlagen vormen een integraal onderdeel van deze DPA.

ARTIKEL 02 Onderwerp, duur en instructies

Verwerker verwerkt Persoonsgegevens voor de aard, doeleinden, duur en categorieën zoals beschreven in Bijlage 1. De verwerking duurt zolang de Hoofdovereenkomst geldt en daarna alleen zolang dit nodig is voor verwijdering, teruggave, wettelijke verplichtingen of de afwikkeling van een geschil.

Verwerker verwerkt Persoonsgegevens uitsluitend op basis van gedocumenteerde instructies van Verwerkingsverantwoordelijke, waaronder de Hoofdovereenkomst, deze DPA, de configuratie van de Diensten en schriftelijke opdrachten van bevoegde contactpersonen.

Als Verwerker op grond van Unierecht of Nederlands recht verplicht is Persoonsgegevens anders te verwerken, informeert Verwerker Verwerkingsverantwoordelijke vooraf, tenzij de wet dit om gewichtige redenen van algemeen belang verbiedt.

Verwerker meldt het onverwijld wanneer een instructie naar zijn gemotiveerde oordeel inbreuk maakt op de AVG of andere toepasselijke gegevensbeschermingswetgeving. Verwerker mag de betreffende uitvoering opschorten totdat de instructie is bevestigd, aangepast of ingetrokken.

ARTIKEL 03 Verplichtingen van Verwerkingsverantwoordelijke

Verwerkingsverantwoordelijke staat ervoor in dat de verwerking rechtmatig is, dat betrokkenen correct zijn geïnformeerd, dat passende grondslagen aanwezig zijn en dat de instructies aan Verwerker rechtmatig, volledig en juist zijn.

Verwerkingsverantwoordelijke beperkt de aangeleverde gegevens tot wat noodzakelijk is, beheert gebruikersrechten zorgvuldig en gebruikt de Diensten niet voor gegevens waarvoor de afgesproken beveiliging en functionaliteit niet passend zijn.

- Verwerkingsverantwoordelijke is primair verantwoordelijk voor verzoeken van betrokkenen, bewaartermijnen en de juistheid van gegevens.
- Bijzondere categorieën van persoonsgegevens en strafrechtelijke gegevens worden alleen verwerkt wanneer dit uitdrukkelijk schriftelijk is overeengekomen en in Bijlage 1 is vastgelegd.
- Verwerkingsverantwoordelijke wijst bevoegde privacy- en securitycontactpersonen aan.

ARTIKEL 04 Geheimhouding en personeel

Verwerker waarborgt dat personen die onder zijn gezag toegang hebben tot Persoonsgegevens deze uitsluitend verwerken op instructie en aan een passende wettelijke of contractuele geheimhoudingsplicht zijn gebonden. Toegang wordt verleend volgens het need-to-know- en least-privilegebeginsel.

Verwerker bevordert passend privacy- en beveiligingsbewustzijn en trekt toegangsrechten tijdig in wanneer een functie of betrokkenheid eindigt.

ARTIKEL 05 Beveiliging

Verwerker treft en onderhoudt passende technische en organisatorische maatregelen als bedoeld in artikel 32 AVG. De maatregelen zijn beschreven in Bijlage 2 en worden afgestemd op de stand van de techniek, uitvoeringskosten, aard, omvang, context en doeleinden van de verwerking en de risico's voor betrokkenen.

Verwerker mag maatregelen wijzigen om technische of organisatorische ontwikkelingen te volgen, mits het overeengekomen beveiligingsniveau niet wezenlijk afneemt.

Verwerkingsverantwoordelijke blijft verantwoordelijk voor het veilig gebruik van de Diensten aan zijn zijde, waaronder endpointbeveiliging, beheer van accounts, sterke authenticatie, autorisaties, API-sleutels, integraties en het tijdig verwijderen van voormalige gebruikers.

ARTIKEL 06 Datalekken

Verwerker stelt Verwerkingsverantwoordelijke zonder onredelijke vertraging en, voor zover redelijkerwijs mogelijk, binnen 24 uur na bevestiging op de hoogte van een Datalek dat betrekking heeft op Persoonsgegevens van Verwerkingsverantwoordelijke. Een eerste melding mag worden aangevuld zodra meer informatie beschikbaar is.

De melding bevat, voor zover bekend: de aard van het Datalek, categorieën en bij benadering aantallen betrokkenen en records, waarschijnlijke gevolgen, getroffen of voorgestelde maatregelen en een contactpunt. Verwerker documenteert relevante feiten, gevolgen en herstelmaatregelen.

Verwerker werkt redelijkerwijs mee zodat Verwerkingsverantwoordelijke zijn meld- en informatieplichten kan beoordelen en nakomen. Verwerker doet geen melding aan een toezichthouder of betrokkenen namens Verwerkingsverantwoordelijke, tenzij schriftelijk opgedragen of wettelijk verplicht.

ARTIKEL 07 Rechten van betrokkenen en ondersteuning

Rekening houdend met de aard van de verwerking helpt Verwerker Verwerkingsverantwoordelijke met passende technische en organisatorische maatregelen bij verzoeken tot inzage, rectificatie, verwijdering, beperking, overdraagbaarheid en bezwaar.

Als een betrokkene zich rechtstreeks tot Verwerker richt over gegevens die namens Verwerkingsverantwoordelijke worden verwerkt, stuurt Verwerker het verzoek zonder inhoudelijke beantwoording door, tenzij Verwerkingsverantwoordelijke anders instrueert.

Verwerker verleent, rekening houdend met de aard van de verwerking en beschikbare informatie, redelijke bijstand bij gegevensbeschermingseffectbeoordelingen, voorafgaande raadplegingen en de naleving van artikelen 32 tot en met 36 AVG.

ARTIKEL 08 Subverwerkers

Verwerkingsverantwoordelijke verleent algemene schriftelijke toestemming voor het inschakelen van de in Bijlage 3 genoemde subverwerkers en voor toekomstige wijzigingen volgens dit artikel.

Verwerker informeert Verwerkingsverantwoordelijke ten minste 30 dagen vooraf over een beoogde toevoeging of vervanging die Persoonsgegevens kan verwerken. Verwerkingsverantwoordelijke kan binnen 14 dagen gemotiveerd bezwaar maken op redelijke privacy- of beveiligingsgronden. Partijen zoeken dan te goeder trouw een oplossing. Als geen redelijke oplossing mogelijk is, mag Verwerkingsverantwoordelijke het direct getroffen onderdeel van de Diensten beëindigen.

Verwerker legt een subverwerker schriftelijk materieel dezelfde gegevensbeschermingsverplichtingen op als in deze DPA en blijft jegens Verwerkingsverantwoordelijke verantwoordelijk voor de uitvoering daarvan.

ARTIKEL 09 Internationale doorgiften

Verwerker verwerkt Persoonsgegevens in beginsel binnen de Europese Economische Ruimte. Een doorgifte naar een derde land vindt alleen plaats als is voldaan aan hoofdstuk V AVG.

Als geen adequaatheidsbesluit geldt, gebruikt Verwerker een geldig doorgiftemechanisme, waaronder waar passend de standaardcontractbepalingen van Uitvoeringsbesluit (EU) 2021/914, en beoordeelt en treft Verwerker zo nodig aanvullende maatregelen. Bij strijdigheid gaan de toepasselijke standaardcontractbepalingen voor.

Externe identiteitsproviders en optionele klantintegraties kunnen gegevens buiten de EER verwerken op initiatief van Verwerkingsverantwoordelijke. De specifieke rollen en doorgiftewaarborgen volgen uit de configuratie, voorwaarden van de betrokken provider en Bijlage 3.

ARTIKEL 10 Audit en informatie

Verwerker stelt op redelijk verzoek informatie beschikbaar die nodig is om naleving van artikel 28 AVG en deze DPA aan te tonen. Verwerker mag daarbij vertrouwelijke informatie, informatie over andere klanten en beveiligingsgevoelige details afschermen.

Verwerkingsverantwoordelijke mag maximaal eenmaal per kalenderjaar en aanvullend na een ernstig Datalek een audit uitvoeren of laten uitvoeren door een onafhankelijke deskundige die aan geheimhouding is gebonden. Een audit wordt ten minste 30 dagen vooraf aangekondigd, vindt tijdens normale werktijden plaats en mag de Diensten niet onredelijk verstoren.

Partijen gebruiken eerst beschikbare rapportages, vragenlijsten, certificaten en externe assurance. Redelijke auditkosten komen voor rekening van Verwerkingsverantwoordelijke, tenzij een materiële tekortkoming van Verwerker wordt vastgesteld.

ARTIKEL 11 Teruggave, verwijdering en bewaartermijnen

Tijdens de looptijd kan Verwerkingsverantwoordelijke gegevens exporteren voor zover de Diensten daarin voorzien. Na beëindiging verwijdert of retourneert Verwerker, naar keuze van Verwerkingsverantwoordelijke, Persoonsgegevens binnen 30 dagen, tenzij een wettelijke bewaarplicht of een schriftelijk overeengekomen langere termijn geldt.

Kopieën in back-ups worden volgens de reguliere back-upcyclus ontoegankelijk gemaakt en uiterlijk binnen 90 dagen overschreven of verwijderd, tenzij technisch of wettelijk een andere termijn noodzakelijk is. Tot verwijdering blijven deze gegevens beschermd en worden zij niet voor andere doeleinden gebruikt.

Gegevens die Verwerker voor eigen doeleinden en onder eigen verantwoordelijkheid verwerkt, zoals de eigen contract- en factuuradministratie, vallen niet onder de verwijderinstructie van dit artikel.

ARTIKEL 12 Kosten

De gebruikelijke uitvoering van deze DPA is inbegrepen in de vergoeding voor de Diensten. Voor buitengewone, omvangrijke of herhaalde bijstand mag Verwerker na voorafgaande afstemming redelijke kosten in rekening brengen, tenzij de bijstand nodig is door een toerekenbare tekortkoming van Verwerker.

ARTIKEL 13 Aansprakelijkheid

De aansprakelijkheidsregeling en beperkingen uit de Hoofdovereenkomst gelden onverkort ook voor deze DPA. De totale aansprakelijkheid van Verwerker op grond van de Hoofdovereenkomst en deze DPA samen is beperkt tot het in de Hoofdovereenkomst genoemde maximum; dit maximum geldt eenmalig en wordt niet verhoogd door meerdere claims of door het bestaan van deze DPA. Niets in deze DPA beperkt rechten van betrokkenen of bevoegdheden van toezichthouders die niet contractueel kunnen worden beperkt.

Iedere Partij is verantwoordelijk voor bestuurlijke boetes voor zover die voortvloeien uit haar eigen handelen of nalaten. Verwerker is niet aansprakelijk voor schade die voortvloeit uit instructies van Verwerkingsverantwoordelijke, uit onrechtmatige of onvolledige gegevens die Verwerkingsverantwoordelijke aanlevert, of uit het niet naleven door Verwerkingsverantwoordelijke van haar eigen verplichtingen onder de AVG. Verwerkingsverantwoordelijke vrijwaart Verwerker voor aanspraken van betrokkenen en derden die daaruit voortvloeien.

ARTIKEL 14 Looptijd en beëindiging

Deze DPA treedt in werking op de Ingangsdatum en geldt zolang Verwerker Persoonsgegevens namens Verwerkingsverantwoordelijke verwerkt. Bepalingen die naar hun aard voortduren, waaronder geheimhouding, audit over de toepasselijke periode, verwijdering en aansprakelijkheid, blijven na beëindiging van kracht.

Als Verwerker wezenlijk of herhaaldelijk tekortschiet in zijn verplichtingen uit deze DPA en de tekortkoming niet binnen een redelijke hersteltermijn verhelpt, mag Verwerkingsverantwoordelijke de verwerking opschorten of de Hoofdovereenkomst voor het getroffen deel beëindigen.

ARTIKEL 15 Toepasselijk recht en geschillen

Op deze DPA is Nederlands recht van toepassing. Geschillen worden behandeld volgens de geschillenregeling in de Hoofdovereenkomst. Als daarin geen bevoegde rechter is aangewezen, worden geschillen voorgelegd aan de bevoegde rechter in het arrondissement waar Verwerker is gevestigd.

Dit artikel laat de wettelijke bevoegdheden van de Autoriteit Persoonsgegevens en andere bevoegde toezichthoudende autoriteiten onverlet.

BIJLAGE 1

Beschrijving van de verwerking

ONDERWERP	Levering, beveiliging, ondersteuning en beheer van de door Verwerkingsverantwoordelijke afgenomen Infaris-diensten, waaronder het centrale platform voor accounts, organisaties, licenties en facturatie en de daarop aangesloten producten.
DUUR	Gedurende de Hoofdovereenkomst, plus de verwijder- en back-uptermijnen uit artikel 11.
AARD VAN DE VERWERKING	Verzamelen, vastleggen, structureren, opslaan, raadplegen, gebruiken, koppelen, verzenden, beveiligen, ondersteunen, exporteren en verwijderen.
DOELEINDEN	Account- en identiteitsbeheer, authenticatie, organisatie- en rollenbeheer, licenties en entitlements, facturatie-ondersteuning, transactionele communicatie, support, beveiliging, logging en levering van gekozen integraties.
FREQUENTIE	Doorlopend en op verzoek van gebruikers, beheerders, gekoppelde producten en geautoriseerde API-clients.

Categorieën betrokkenen

- Gebruikers, medewerkers, beheerders, opdrachtnemers en vertegenwoordigers van Verwerkingsverantwoordelijke.
- Uitgenodigde gebruikers en contactpersonen van organisaties of klanten die door Verwerkingsverantwoordelijke worden beheerd.
- Contactpersonen voor facturatie, support, security en zakelijke communicatie.
- Bezoekers en eindgebruikers voor zover hun technische gegevens in logs of beveiligingsregistraties voorkomen.

Categorieën persoonsgegevens

CATEGORIE	VOORBEELDEN
Identiteit en contact	Naam, e-mailadres, gebruikersnaam, profielfoto, telefoon, functie, taalvoorkeur.
Organisatie en relatie	Organisatienaam, rol, lidmaatschap, domein, uitnodigingen, relatie- en contactgegevens, adres, KVK- en btw-nummer.
Authenticatie en beveiliging	Account-ID's, sessies, passkeymetadata, MFA-status, versleutelde TOTP-secret, gehashte back-upcodes, OAuth-tokens, authenticatie- en auditgebeurtenissen, IP-adres.
Licentie en transactie	Plan, licenties, activaties, klant- en abonnementsreferenties, betaalstatus en Stripe-identificatoren. Infaris bewaart zelf geen volledige betaalkaartgegevens.

CATEGORIE	VOORBEELDEN
Techniek en gebruik	Browser- en apparaatgegevens, timestamps, verzoekmetadata, logs, configuraties, API- en webhookgebeurtenissen, gekozen integraties.
Support en communicatie	Supportberichten, incidentinformatie, e-mailbezorggegevens en inhoud die de klant voor ondersteuning verstrekt.

Bijzondere gegevens en beperkingen

De Diensten zijn niet bedoeld voor de structurele verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9 AVG of strafrechtelijke gegevens als bedoeld in artikel 10 AVG. Verwerkingsverantwoordelijke voert dergelijke gegevens niet in zonder voorafgaande schriftelijke overeenkomst en passende aanvullende maatregelen.

BIJLAGE 2

Technische en organisatorische maatregelen

RISICOGEBASEERDE MAATREGELEN

De onderstaande maatregelen beschrijven het overeengekomen basisniveau. De precieze inrichting kan wijzigen wanneer techniek of risico's veranderen, zonder wezenlijke verlaging van het beschermingsniveau.

DOMEIN	MAATREGELEN
Governance	Vastgelegde rollen en autorisaties; vertrouwelijkheid; periodieke beoordeling van toegang; incident- en datalekprocedure; beheer van wijzigingen en kwetsbaarheden.
Identiteit en toegang	Passwordless authenticatie waar beschikbaar; passkeys/WebAuthn; TOTP-MFA en back-upcodes; OAuth 2.0/OpenID Connect; sessiebeheer; rolgebaseerde toegang; least privilege; logging van beheerdershandelingen en impersonatie.
Cryptografie	TLS voor gegevens tijdens transport; versleuteling van gevoelige secrets en SSO-configuraties; wachtwoorden uitsluitend als sterke hash waar de demofunctie dit vereist; ondertekende webhooks en validatie van tokens.
Applicatiebeveiliging	Content Security Policy en gangbare securityheaders; bescherming tegen CSRF, rate limiting, botbescherming via Cloudflare Turnstile, validatie van invoer, veilige secretopslag en afhankelijkhedenbeheer.
Infrastructuur	Productie- en ontwikkelomgevingen gescheiden; containerized deployment; netwerktoegang beperkt; database niet vrij toegankelijk voor het publieke internet; HTTPS-afdwinging; firewall- en DDoS/WAF-bescherming.
Beschikbaarheid	Back-ups en herstelprocedures; monitoring van dienstgezondheid; incidentrunbook; gecontroleerde deployments en rollbackmogelijkheid; rate limiting om misbruik en overbelasting te beperken.
Logging en detectie	Authenticatie-, audit- en relevante operationele logs; monitoring op afwijkingen en fouten; beveiligde meldkanalen voor incidenten; logs worden beperkt tot wat operationeel en beveiligingstechnisch nodig is.
Dataminimalisatie	Gescheiden tenant- en organisatiescope; beperkte gegevensvelden; geen opslag van volledige betaalkaartgegevens; export en verwijdering op verzoek; bewaartermijnen afgestemd op doel en wettelijke plichten.
Leveranciersbeheer	Beoordeling van relevante leveranciers; schriftelijke gegevensbeschermingsvoorwaarden; beperkte gegevensverstrekking; passende doorgiftewaarborgen voor verwerking buiten de EER.
Continu verbeteren	Regelmatige evaluatie van risico's, maatregelen en incidenten; herstel van vastgestelde tekortkomingen; beveiligingsinformatie beschikbaar voor zakelijke klanten binnen redelijke vertrouwelijkheidsgrenzen.

BIJLAGE 3

Subverwerkers

Onderstaande lijst is gebaseerd op de huidige Infaris-architectuur. Alleen leveranciers die voor de door de klant gebruikte functies daadwerkelijk Persoonsgegevens ontvangen, gelden voor die klant als subverwerker. De actuele contractuele configuratie en hostingregio zijn leidend.

LEVERANCIER / DIENST	DOEL EN GEGEVENS	LOCATIE / WAARBORG
Hosting- en datacenterleverancier van IMDigital	Hosting van de Infaris-applicaties en operationele metadata.	Nederland / EER. Definitieve leverancier en locatie invullen vóór ondertekening.
PostgreSQL-infrastructuur van IMDigital	Primaire opslag van account-, organisatie-, relatie-, licentie-, authenticatie- en auditgegevens.	Nederland / EER; self-hosted database-infrastructuur.
Redis Cloud / Redis Labs	Rate limiting en tijdelijke technische sleutels; geen beoogde duurzame inhoudsopslag.	Regio volgens productieconfiguratie. DPA en, indien nodig, SCC's.
Stripe	Betalingen, abonnementen, facturatie- en klantreferenties. Volledige kaartgegevens worden door Stripe verwerkt.	EER en mogelijk derde landen volgens Stripe DPA; adequaatheidsbesluit of SCC's waar nodig.
Resend	Verzending van transactionele e-mail, zoals magic links, activatie, uitnodigingen en serviceberichten.	Regio volgens accountconfiguratie; DPA en passend doorgiftemechanisme waar nodig.
Cloudflare	DNS, CDN/WAF, DDoS-bescherming en Turnstile-botdetectie; IP- en verzoekmetadata.	Wereldwijd netwerk; Cloudflare DPA en adequaatheidsbesluit of SCC's waar nodig.
Microsoft / Google, optioneel	Federatieve authenticatie wanneer de klant of gebruiker deze provider kiest; accountidentificatoren en tokens.	Volgens provider en tenantconfiguratie; vaak afzonderlijke verwerkingsverantwoordelijke, anders DPA en doorgiftewaarborg.
Notion, optioneel intern	Changelog- of relatieondersteuning wanneer deze koppeling in de productieconfiguratie is ingeschakeld.	Alleen indien geactiveerd; DPA en passend doorgiftemechanisme waar nodig.
Slack, optioneel intern	Operationele beveiligings- en supportmeldingen. Geen structurele opslag van volledige klantdatasets beoogd.	Alleen indien geactiveerd; DPA en passend doorgiftemechanisme waar nodig.

Wijzigingsbericht

Kennisgevingen over materiële wijzigingen in subverwerkers worden verzonden naar het privacy- of contractcontact van Verwerkingsverantwoordelijke of gepubliceerd via een overeengekomen klantkanaal. Verwerkingsverantwoordelijke houdt deze contactgegevens actueel.

BIJLAGE 4

Contacten, keuzes en ondertekening

PRIVACYCONTACT KLANT	[NAAM, FUNCTIE, E-MAIL EN TELEFOON]
SECURITYCONTACT KLANT	[NAAM, FUNCTIE, E-MAIL EN TELEFOON]
PRIVACYCONTACT INFARIS	privacy@infaris.com
JURIDISCH CONTACT INFARIS	legal@infaris.com
BEVEILIGINGSMELDINGEN	info@infaris.com, tenzij schriftelijk een specifiek incidentadres is verstrekt
KEUZE NA EINDE OVEREENKOMST	☐ verwijderen ☐ retourneren/exporteren, daarna verwijderen
AFWIJKENDE BEWAARTERMIJN	[NIET VAN TOEPASSING / SPECIFICATIE]
TOEGESTANE BIJZONDERE GEGEVENS	Geen, tenzij hier uitdrukkelijk gespecificeerd: [SPECIFICATIE]

Ondertekening

Partijen verklaren bevoegd te zijn en stemmen door ondertekening in met deze DPA en alle bijlagen.

VERWERKINGSVERANTWOORDELIJKE	VERWERKER
[NAAM KLANT]	**IMDigital, handelend onder de naam Infaris**
Naam	Naam
Functie	Functie
Plaats	Plaats
Datum	Datum
Handtekening	Handtekening

Juridische referenties

AVG, Verordening (EU) 2016/679

Standaardcontractbepalingen, Uitvoeringsbesluit (EU) 2021/914

EDPB Guidelines 07/2020 over verwerkingsverantwoordelijken en verwerkers