Versie: 1.0 / 1 december 2026

Verwerkers-overeenkomst Helios IT

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

NLdigital versie maart 2025

Deel 1: Data Pro Statement

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

Algemene informatie

1. **Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):**
   Helios IT Solutions B.V., Schipluidenlaan 4, 1062 HE Amsterdam, KvK-nummer 68332289.
   Voor vragen over dit Data Pro Statement of dataprotectie kan contact worden opgenomen via privacy@helios-it.nl of +31 20 802 8000.

2. **Dit Data Pro Statement geldt vanaf 1 december 2026, versie 1.0.**
   Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van dataprotectie voorbereid en actueel te blijven. Wij informeren opdrachtgevers over nieuwe versies via onze normale communicatiekanalen, waaronder per e-mail of via de klantomgeving.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor:** Managed IT-dienstverlening; levering, inrichting en beheer van Microsoft 365 en Google Workspace; servicedesk, monitoring en beheer via RMM; endpointbeveiliging en EDR/MDR; back-up- en hersteloplossingen; cloud-, hosting- en domeindiensten; migraties van e-mail-, server-, on-premises- en cloudomgevingen; ontwikkeling en beheer van apps, dashboards en andere klantspecifieke systemen; AI-gerelateerde diensten, implementaties en ondersteuning; en overige IT-diensten die in de Overeenkomst met Opdrachtgever zijn vastgelegd.

4. **Omschrijving product(en)/dienst(en)**
   Helios IT Solutions B.V. levert als one-stop IT-dienstverlener zakelijke IT-oplossingen. De dienstverlening omvat onder meer levering van licenties en diensten, inrichting, beheer, beveiliging, monitoring, ondersteuning, hosting, back-up, herstel, migratie en ontwikkeling van IT-omgevingen en klantspecifieke oplossingen. In de Overeenkomst, offerte of SLA met Opdrachtgever is bepaald welke diensten worden afgenomen.

5. **Beoogd gebruik**
   De producten en diensten zijn ontworpen en ingericht voor het verwerken van naam-, adres- en contactgegevens; zakelijke en organisatorische gegevens; account-, gebruikers-, identificatie-, authenticatie- en autorisatiegegevens; communicatiegegevens, waaronder e-mail en agenda; document-, bestands- en applicatiegegevens; technische gegevens, zoals IP-adressen, apparaat-, netwerk-, log- en telemetriegegevens; back-up- en herstelgegevens; en overige persoonsgegevens die Opdrachtgever opslaat of verwerkt binnen de geleverde of beheerde systemen. De betrokkenen kunnen onder meer medewerkers, ingehuurde krachten, sollicitanten, klanten, leveranciers, zakelijke contacten en gebruikers van systemen, websites, applicaties en portals van Opdrachtgever zijn, alsmede overige personen van wie Opdrachtgever persoonsgegevens verwerkt binnen de door Helios IT geleverde of beheerde IT-omgeving.

- De dienstverlening is niet specifiek gericht op de verwerking van bijzondere categorieën van persoonsgegevens, strafrechtelijke persoonsgegevens of door de overheid uitgegeven persoonsnummers. Afhankelijk van de gegevens die Opdrachtgever in de geleverde of beheerde systemen verwerkt, kunnen dergelijke gegevens hiervan wel onderdeel uitmaken.
  Het verwerken van deze gegevens met de hiervoor omschreven producten of diensten is ter beoordeling en verantwoordelijkheid van Opdrachtgever. Opdrachtgever bepaalt welke gegevens binnen de geleverde of beheerde systemen worden verwerkt.

6. **Privacy by design/privacy by default**
   Helios IT Solutions B.V. houdt bij de inrichting en uitvoering van de dienstverlening, voor zover passend bij de aard en omvang van de opdracht, rekening met privacy by design en privacy by default. Helios IT past daarbij onder meer passende toegangsbeveiliging, autorisaties, logging, versleuteling en standaardinstellingen toe. De uiteindelijke configuratie en inrichting kunnen mede afhankelijk zijn van de keuzes en instructies van Opdrachtgever.

7. **Data processor gebruikt de Standaardclausules voor verwerkingen, welke als Deel 2 bij dit Data Pro Statement zijn opgenomen en samen met dit Data Pro Statement de verwerkersovereenkomst vormen.**

8. **Data processor kan persoonsgegevens (gedeeltelijk) buiten de EU/EER verwerken. Voor zover daarbij sprake is van doorgifte naar een derde land, wordt een passend beschermingsniveau geborgd door een geldige doorgiftegrondslag conform de AVG, zoals een adequaatheidsbesluit van de Europese Commissie of de Standard Contractual Clauses (SCC's), zo nodig aangevuld met passende aanvullende maatregelen.**

9. **Data processor maakt gebruik van de volgende sub-processors:**
   Data processor maakt gebruik van de volgende sub-processors:
   • Microsoft (Microsoft 365, Azure, Entra ID en Copilot): verwerking binnen de EU/EER en, afhankelijk van de dienst en ondersteuning, mogelijk in derde landen; passende waarborgen overeenkomstig de toepasselijke Microsoft-verwerkersvoorwaarden.
   • Google (Google Workspace): verwerking binnen de EU/EER en mogelijk in derde landen; passende waarborgen overeenkomstig de toepasselijke Google-verwerkersvoorwaarden.
   • Hetzner Online GmbH (VPS-hosting en cloudopslag): verwerking binnen de EU/EER.
   • Realtime Register B.V. (domeinregistratie en -beheer): verwerking binnen de EU/EER.
   • NinjaOne (RMM, monitoring en SaaS-back-up): verwerking binnen de EU/EER en mogelijk in derde landen; passende waarborgen overeenkomstig de toepasselijke verwerkersvoorwaarden.
   • SentinelOne (endpointbeveiliging, EDR en MDR): verwerking binnen de EU/EER en mogelijk in derde landen; passende waarborgen overeenkomstig de toepasselijke verwerkersvoorwaarden.
   • Anthropic (Claude en AI-gerelateerde dienstverlening): verwerking mogelijk in derde landen; passende waarborgen overeenkomstig de toepasselijke verwerkersvoorwaarden.
   De daadwerkelijk ingezette sub-processors zijn afhankelijk van de door Opdrachtgever afgenomen diensten. Data processor informeert Opdrachtgever overeenkomstig de Standaardclausules over relevante wijzigingen.

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
Helios IT Solutions B.V. ondersteunt Opdrachtgever op redelijk en schriftelijk verzoek bij de afhandeling van verzoeken van betrokkenen, voor zover de benodigde handelingen niet zelfstandig door Opdrachtgever kunnen worden uitgevoerd. Indien een betrokkene zich rechtstreeks tot Helios IT wendt, wordt deze in beginsel doorverwezen naar Opdrachtgever. Eventuele werkzaamheden kunnen als meerwerk tegen de overeengekomen of gebruikelijke tarieven in rekening worden gebracht.

11. **Data processor zal op de volgende wijze medewerking verlenen aan Data Protection Impact Assessments (DPIA):**
Indien Opdrachtgever verplicht is een Data Protection Impact Assessment (DPIA) uit te voeren, verleent Helios IT Solutions B.V. na een redelijk en schriftelijk verzoek passende medewerking voor zover de gevraagde informatie en ondersteuning betrekking hebben op de door Helios IT uitgevoerde verwerking. Eventuele werkzaamheden kunnen als meerwerk tegen de overeengekomen of gebruikelijke tarieven in rekening worden gebracht.

12. **Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen drie maanden, zodat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn, tenzij anders overeengekomen of een wettelijke bewaarplicht geldt.**
Voor persoonsgegevens in back-ups, logbestanden en archieven geldt dat deze volgens de reguliere bewaartermijnen en verwijdercycli van de betreffende oplossing worden verwijderd. Gedurende deze periode worden deze gegevens niet voor andere doeleinden verwerkt.

13. **Retourneren van persoonsgegevens na beëindiging van de Overeenkomst**
Op schriftelijk verzoek van Opdrachtgever stelt Helios IT Solutions B.V., voor zover technisch redelijkerwijs mogelijk, de persoonsgegevens beschikbaar in een gangbaar formaat dat past bij de betreffende dienst. Werkzaamheden voor export, overdracht of migratie kunnen als meerwerk tegen de overeengekomen of gebruikelijke tarieven in rekening worden gebracht.

Beveiligingsbeleid

14. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
Helios IT Solutions B.V. treft, rekening houdend met de aard van de dienstverlening, de verwerkingsrisico's, de stand van de techniek en de gebruikte platforms, passende technische en organisatorische beveiligingsmaatregelen. Deze omvatten onder meer:
• beperking van toegang tot medewerkers die deze voor hun werkzaamheden nodig hebben;
• centraal en beveiligd beheer van beheeraccounts en toegangsgegevens, onder meer via een wachtwoordkluis;
• toepassing van multi-factor authenticatie waar beschikbaar en passend;
• toepassing van versleuteling tijdens opslag en transport waar passend, mede via de beveiligingsvoorzieningen van gebruikte platforms en sub-processors;
• logging van aanmeldingen en beheeractiviteiten binnen de voornaamste beheerplatforms, zodat relevante

handelingen en toegang achteraf kunnen worden onderzocht;
• automatische uitvoering en monitoring van back-uptaken, met meldingen wanneer taken niet of niet succesvol worden uitgevoerd;
• gebruik van versiebeheer, snapshots, redundantie en bestandssysteemvoorzieningen waar de gekozen oplossing daarin voorziet;
• toepassing van beveiligingsupdates en patches op systemen die onder beheer van Helios IT vallen, waar passend en mede via geautomatiseerde beheer- en monitoringvoorzieningen;
• contractuele geheimhouding voor medewerkers die toegang kunnen hebben tot persoonsgegevens; en
• interne opvolging en onderzoek van geconstateerde beveiligingsincidenten en mogelijke datalekken.
Helios IT beoordeelt en verbetert deze maatregelen op basis van ontwikkelingen, incidenten, geconstateerde risico's en wijzigingen in de dienstverlening. De concrete maatregelen kunnen per dienst en klantomgeving verschillen.

15. **Data processor beschikt op de ingangsdatum van dit Data Pro Statement niet over een formeel gecertificeerd Information Security Management System (ISMS).**

16. **Data processor beschikt op de ingangsdatum van dit Data Pro Statement niet over externe informatiebeveiligings- of privacycertificeringen.**

Datalekkenprotocol

17. **In geval er toch iets mis gaat, hanteert data processor het volgende datalekkenprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**
Helios IT Solutions B.V. informeert Opdrachtgever zonder onredelijke vertraging nadat Helios IT kennis heeft genomen van een inbreuk in verband met persoonsgegevens die in het kader van de dienstverlening voor Opdrachtgever worden verwerkt. Helios IT verstrekt daarbij, voor zover beschikbaar, de informatie die Opdrachtgever redelijkerwijs nodig heeft om het incident te beoordelen en aan eventuele wettelijke meldverplichtingen te voldoen. Beveiligingsincidenten en mogelijke datalekken worden na constatering intern zo spoedig mogelijk onderzocht, beperkt en opgevolgd. Meldingen worden gedaan via de bij Helios IT bekende contactgegevens van Opdrachtgever. Voor urgente afstemming kan contact worden opgenomen via privacy@helios-it.nl of +31 20 802 8000.

Deel 2: Standaardclausules voor verwerkingen

Versie: maart 2025

Vormt samen met het Data Pro Statement de verwerkersovereenkomst en is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden.

Artikel 1. Definities

Onderstaande begrippen hebben in deze Standaardclausules voor verwerkingen, in het Data Pro Statement en in de overeenkomst de volgende betekenis:

1.1 **Autoriteit Persoonsgegevens (AP):** toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 AVG.
1.2 **AVG:** de Algemene verordening gegevensbescherming.
1.3 **Data Processor**: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.
1.4 **Data Pro Statement**: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, sub-processors, datalekken, certificeringen en omgang met rechten van Data subjects.
1.5 **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon.
1.6 **Opdrachtgever:** partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.
1.7 **Overeenkomst**: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.
1.8 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 AVG, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.
1.9 **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 AVG.

Artikel 2. Algemeen

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.
2.2 Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.
2.3 Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.

2.4 Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de AVG, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de AVG en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de AVG zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de AVG handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor.

Artikel 3. Beveiliging

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico's en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten of door de overheid uitgegeven persoonsnummers.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

Artikel 4. Inbreuken in verband met Persoonsgegevens

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 AVG) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

4.2 Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 AVG moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 AVG.

4.4 Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

Artikel 5. Geheimhouding

5.1 Data Processor waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

Artikel 6. Looptijd en beëindiging

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

6.2 Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen aan Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de AVG is ten aanzien van de Persoonsgegevens.

Artikel 7. Rechten Data subjects, Data Protection Impact Assessment (DPIA) en Auditrechten

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 AVG.

7.3 Data Processor zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

7.4 Data Processor kan desgewenst de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of een daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige, indien hij over een dergelijk certificaat of auditrapport beschikt.

7.5 Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de AVG of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.6 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.7 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

Artikel 8. Sub-Processors

8.1 Data Processor heeft in het Data Pro Statement vermeld of, en zo ja welke derde partijen (sub-processors of subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere sub-processors in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

8.3 Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

Artikel 9. Overig

Deze Standaardclausules voor verwerkingen vormen tezamen met het Data Pro Statement een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst.