Versie: v1.0 / 22-09-2026

Verwerkers-overeenkomst Lakeglide

Bos & Brouwer B.V

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

NLdigital versie maart 2025

Deel 1: Data Pro Statement

Deel 1 van de verwerkersovereenkomst van Bos & Brouwer B.V. voor Lakeglide vormt samen met de Standaardclausules voor verwerkingen (NLdigital, maart 2025) de verwerkersovereenkomst.

Algemene informatie

1. **Dit Data Pro Statement is opgesteld door de volgende Data Processor (verwerker)**

   Bos & Brouwer B.V. (KvK 99201089), Spiegeltuin 1, 5223 MZ 's-Hertogenbosch. Lakeglide is een handelsnaam van Bos & Brouwer B.V.

   Voor vragen over dit Data Pro Statement of over dataprotectie kan contact worden opgenomen met Roel Knitel, privacy@lakeglide.com.

2. **Dit Data Pro Statement geldt vanaf 22-09-2026 (v1.0)**

   Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van dataprotectie voorbereid en actueel te blijven. Nieuwe versies kondigen wij per e-mail aan bij de door Opdrachtgever opgegeven beheerder van de omgeving.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van Data Processor**

   Lakeglide, waaronder begrepen alle onderdelen die onder die naam worden geleverd, inclusief het gebruik tijdens een proefperiode.

4. **Omschrijving product(en)/dienst(en)**

   Lakeglide is een managed dataplatform waarmee Opdrachtgever brondata ontsluit, modelleert en analyseert ten behoeve van stuurinformatie. Het platform wordt gehost in de Azure-tenant van Data Processor. Iedere Opdrachtgever beschikt over een eigen Databricks-workspace en een eigen storage account.

5. **Beoogd gebruik**

   Het product is ontworpen en ingericht voor de verwerking van persoonsgegevens in het kader van gegevensopslag, gegevensverwerking en gegevensanalyse.

Het product is ontworpen en ingericht om de volgende soorten gegevens te verwerken:

- identificatiegegevens (zoals naam, gebruikersnaam of klantnummer);
- contactgegevens (zoals e-mailadres, telefoonnummer en adresgegevens);
- organisatorische of functierelaties (zoals functietitel of afdeling);
- klant- of relatiegegevens;
- transactiegegevens;
- locatiegegevens;
- gebruiksgegevens en loggegevens die ontstaan door het gebruik van het platform.

Deze gegevens kunnen betrekking hebben op de volgende categorieën betrokkenen:

- gebruikers van het platform;
- contactpersonen bij klanten, relaties en leveranciers van Opdrachtgever;
- medewerkers van Opdrachtgever, voor zover zij in de brondata voorkomen.

Bij het ontwerp en de inrichting van het product is in beginsel geen rekening gehouden met de verwerking van bijzondere categorieën van persoonsgegevens, gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers, tenzij uitdrukkelijk anders overeengekomen in een specifieke opdracht of module. Het gebruik van het product voor de verwerking van dergelijke gegevens geschiedt onder verantwoordelijkheid en beoordeling van Opdrachtgever.

De standaardconnectoren en veldmappings zijn zo ingericht dat velden die bedoeld zijn voor door de overheid uitgegeven persoonsnummers of bijzondere persoonsgegevens niet worden overgenomen. Opdrachtgever blijft verantwoordelijk voor de inhoud van de door hem ontsloten brondata, waaronder gegevens die voorkomen in vrije tekstvelden of in velden die afwijkend van hun oorspronkelijke doel worden gebruikt.

6. Privacy by design/privacy by default

Persoonsgegevens worden verwerkt binnen de Azure-tenant van Data Processor. Iedere Opdrachtgever beschikt over een eigen Databricks-workspace en een eigen storage account, waardoor gegevens van verschillende Opdrachtgevers gescheiden blijven.

Voor alle gegevens wordt standaard encryptie toegepast, zowel tijdens opslag als tijdens transport.

In de standaardmapping van de connectoren worden daartoe aangewezen kolommen gemaskeerd.

Toegang tot de omgeving van Opdrachtgever is beperkt tot geautoriseerde personen en systemen op basis van het need-to-know-principe, en vindt uitsluitend plaats voor beheer, onderhoud en de afhandeling van supportverzoeken. Alle toegang tot en het gebruik van persoonsgegevens wordt gemonitord en gelogd ten behoeve van beveiliging, controle en incidentdetectie.

7. Standaardclausules

Data Processor gebruikt de Standaardclausules voor verwerkingen (NLdigital, versie maart 2025), welke als bijlage bij de Overeenkomst te vinden zijn.

8. Dataverwerking binnen EU/EER

Data Processor verwerkt de persoonsgegevens van zijn Opdrachtgevers binnen de EU/EER, in de Azure-regio West Europe, tenzij met Opdrachtgever schriftelijk een andere regio is overeengekomen. Een uitzondering vormt de accountmetadata van platformgebruikers, zie item 9.

Voor de zogeheten Designated Services van Databricks, waaronder de AI-functionaliteit, is verwerking buiten de geografie van de workspace uitgeschakeld en wordt verwerking binnen die geografie op workspaceniveau afgedwongen.

9. Gebruik sub-processors

Data Processor kan bij de uitvoering van de dienstverlening gebruikmaken van sub-processors. Opdrachtgever verleent hierbij algemene toestemming voor het inschakelen van de hieronder genoemde subverwerkers. Wijzigingen worden aangekondigd via een aangepast Data Pro Statement, waarbij Opdrachtgever het recht heeft bezwaar te maken.

Subverwerker	Rol	Binnen EU/EER	Waarborgen
Microsoft Azure	Cloudinfrastructuur, opslag (ADLS Gen2), compute, Key Vault	Ja	Microsoft DPA, EU Data Boundary, encryptie at rest en in transit, ISO 27001, SOC 1/2, SCC's
Databricks	Dataverwerkingsplatform (notebooks, jobs, Unity Catalog, clusters, Genie)	Deels*	Databricks DPA met SCC's, ISO 27001, SOC 2 Type II, EU-US Data Privacy Framework. Zie voetnoot *
Microsoft Entra ID en Entra External ID	Identiteits- en toegangsbeheer voor interne en externe gebruikers	Ja	Onderdeel Microsoft DPA, RBAC, Conditional Access, EU Data Boundary
Azure Monitor / Log Analytics	Logging, monitoring en audit trails	Ja	Onderdeel Microsoft DPA, versleuteld, RBAC, data in de gekozen Azure-regio
Vercel	Hosting van de webapplicatie	Ja**	DPA met SCC's
Neon	Applicatiedatabase	Ja**	DPA met SCC's
Resend	Transactionele e-mail (inloglinks, meldingen)	Ja**	DPA met SCC's

** De klantdata blijft opgeslagen in de Azure-regio West Europe, tenzij met Opdrachtgever schriftelijk een andere regio is overeengekomen. De accountmetadata van platformgebruikers, zoals naam en e-mailadres, wordt door Azure Databricks ten behoeve van account- en toegangsbeheer ook in de Verenigde Staten opgeslagen. Databricks dekt deze doorgifte af via de Databricks Data Processing Addendum, waarin de EU Standard Contractual Clauses (SCCs) zijn opgenomen.*

*** Deze partijen zijn in de Verenigde Staten gevestigd en leveren hun dienst vanuit een EU-regio. Eventuele doorgifte buiten de EER, bijvoorbeeld in het kader van ondersteuning, wordt afgedekt*

door de met deze partijen overeengekomen SCCs.

10. Ondersteuning Opdrachtgever bij verzoeken van betrokkenen

Opdrachtgever voert zelf de beoordeling van het verzoek en de identificatie van de betrokkene uit, en verwerkt het verzoek eerst in de bronsystemen. Verwijdering of correctie in het lake zonder voorafgaande verwerking in de bron heeft geen blijvend effect, omdat de gegevens bij een volgende load opnieuw worden ingelezen.

Na instructie van Opdrachtgever verwijdert of anonimiseert Data Processor de betreffende gegevens in de historie binnen het platform. Data Processor doet dit binnen twintig werkdagen na ontvangst van de instructie, rekening houdend met de aard en complexiteit van het verzoek.

Alle communicatie met betrokkenen verloopt uitsluitend via Opdrachtgever. Data Processor heeft geen direct contact met betrokkenen en voert geen zelfstandige verificatie uit van hun identiteit.

Indien een supportovereenkomst van toepassing is, vallen de kosten voor deze ondersteuning onder de daarin gemaakte afspraken. In andere gevallen kan ondersteuning worden geleverd tegen het reguliere tarief van Data Processor.

11. Data Protection Impact Assessments

Data Processor verleent op redelijk gegeven verzoek van Opdrachtgever medewerking aan een verplichte DPIA die betrekking heeft op het gebruik van het platform en de bijbehorende dienstverlening.

Deze medewerking bestaat uit het verstrekken van relevante informatie over de werking van de dienstverlening, de technische inrichting, de verwerkingsactiviteiten en de getroffen technische en organisatorische beveiligingsmaatregelen, voor zover deze informatie redelijkerwijs beschikbaar is bij Data Processor.

De medewerking is beperkt tot informatieverstrekking en houdt geen actieve deelname in aan het opstellen, beoordelen of afronden van de DPIA. Opdrachtgever blijft volledig verantwoordelijk voor de uitvoering en de uitkomsten daarvan.

De ondersteuning wordt eenmalig per verplichte DPIA geleverd, op basis van een redelijke inspanningsverplichting en zonder garantie ten aanzien van de uitkomst.

12. Verwijderen persoonsgegevens bij beëindiging

Na beëindiging van de Overeenkomst verwijdert Data Processor alle persoonsgegevens die hij voor Opdrachtgever verwerkt binnen dertig dagen, op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn. Indien Opdrachtgever een overstap heeft ingezet, gaat deze termijn in na afloop van de periode waarin Opdrachtgever zijn gegevens nog kon opvragen.

De verwijdering omvat het volledige storage account van Opdrachtgever en de bijbehorende Databricks-workspace. Historische versies van gegevens blijven binnen het platform maximaal zeven dagen beschikbaar via Delta time travel en worden daarna automatisch opgeruimd.

13. Retourneren persoonsgegevens bij beëindiging

Op verzoek van Opdrachtgever levert Data Processor de gegevens aan in een machineleesbaar formaat, naar keuze als CSV- of Excel-bestand, of via Delta Sharing indien Opdrachtgever over een eigen Databricks-omgeving beschikt.

Data Processor ondersteunt Opdrachtgever bij een overstap naar een andere aanbieder of naar een eigen omgeving. De overstap vindt plaats binnen een overgangsperiode van maximaal dertig dagen na het einde van de opzegtermijn, tenzij dit technisch niet mogelijk is en Data Processor dat onderbouwt. Na afloop van die periode kan Opdrachtgever zijn gegevens nog minimaal dertig dagen opvragen.

Beveiligingsbeleid

14. Beveiligingsmaatregelen

Data Processor heeft passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies, onbevoegde toegang en onrechtmatige verwerking. Deze maatregelen zijn afgestemd op de aard van de dienstverlening en het type persoonsgegevens dat wordt verwerkt.

Pseudonimisering. Gegevens worden niet standaard gepseudonimiseerd. In de standaardmapping van de connectoren worden daartoe aangewezen kolommen gemaskeerd, zodat deze niet in herleidbare vorm in het platform terechtkomen.

Versleuteling. Gegevens worden versleuteld opgeslagen en versleuteld getransporteerd.

Vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht. Iedere Opdrachtgever beschikt over een eigen Databricks-workspace en een eigen storage account. De dienstverlening is beveiligd met een afgezonderde netwerkomgeving. Toegang is beperkt tot geautoriseerde personen en systemen op basis van het need-to-know-principe en wordt gemonitord en gelogd. Beveiligingsincidenten en kwetsbaarheden worden opgevolgd volgens de interne security- en incidentmanagementprocedures van Data Processor.

Herstel na een incident. Het platform bevat gegevens die zijn afgeleid uit de bronsystemen van Opdrachtgever. Die bronsystemen blijven het systeem van vastlegging. Herstel vindt plaats door het terugdraaien van gegevens via Delta time travel binnen een venster van zeven dagen, of door een volledige herlaad vanuit de bronsystemen. Daarnaast wordt gebruikgemaakt van de redundantie van Azure Storage.

15. Information Security Management System

Data Processor hanteert een gestructureerde aanpak voor informatiebeveiliging, vastgelegd in interne procedures en deels geborgd via de gebruikte platformen en technologieën. Data Processor heeft zich geconformeerd aan het ISMS van NLdigital.

Daarnaast werkt Data Processor aan het verkrijgen van een ISO/IEC 27001-certificering. Tot het moment van certificering baseert Data Processor zijn beveiligingsmaatregelen op de

uitgangspunten en best practices van die norm. Op verzoek van Opdrachtgever kan Data Processor nadere toelichting geven over de voortgang van dit traject.

Dit kader wordt periodiek geëvalueerd en waar nodig aangepast.

16. Labels en certificaten

Data Processor beschikt op dit moment niet over labels of certificaten. Zie item 15 voor het lopende ISO/IEC 27001-traject.

Datalekkenprotocol

17. Datalekkenprotocol

Data Processor hanteert een datalekkenprotocol voor het signaleren, beoordelen en afhandelen van beveiligingsincidenten en datalekken die betrekking hebben op de verwerking van persoonsgegevens in het kader van de dienstverlening.

Indien Data Processor kennisneemt van een vermoedelijk datalek, beoordeelt hij onverwijld of sprake is van een inbreuk in verband met persoonsgegevens. Is dat het geval, dan informeert Data Processor Opdrachtgever binnen achtenveertig uur na ontdekking. De melding gaat naar de door Opdrachtgever opgegeven privacycontactpersoon en bevat ten minste:

- de aard van het incident;
- de categorieën persoonsgegevens en betrokkenen waarop het incident betrekking heeft;
- de geschatte omvang van het incident;
- de getroffen en voorgenomen maatregelen;
- een contactpunt bij Data Processor voor nadere informatie.

Het protocol voorziet in maatregelen gericht op het beperken van de gevolgen van het incident, het treffen van corrigerende maatregelen en het voorkomen van herhaling. Incidenten worden vastgelegd en geëvalueerd.

Data Processor verleent, voor zover redelijk, ondersteuning aan Opdrachtgever bij het afhandelen van datalekken, waaronder het verstrekken van aanvullende informatie zodra die beschikbaar komt. Data Processor doet zelf geen meldingen aan de Autoriteit

Persoonsgegevens of aan betrokkenen. Het al dan niet melden blijft de verantwoordelijkheid van Opdrachtgever.

Aanvaarding

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen (NLdigital, versie maart 2025) de verwerkersovereenkomst. De verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en treedt in werking op het moment dat de Overeenkomst tot stand komt.

Aanvaarding vindt elektronisch plaats bij het aangaan van de Overeenkomst. Van iedere aanvaarding legt Data Processor vast: het versienummer van dit Data Pro Statement en van de Standaardclausules, de datum en het tijdstip van aanvaarding, en de identificatie van de omgeving of het account van Opdrachtgever.

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.