



# STANDAARD VERWERKERS- OVEREENKOMST

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Versie januari 2018

# DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkerovereenkomst 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:

Officelynq B.V., Laan van Ypenburg 88, 2497GB 's-Gravenhage

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met: Q. Li, email: [security@officelynq.com](mailto:security@officelynq.com), tel: +31615285737

### 2. Dit Data Pro Statement geldt vanaf 08-10-2019 en betreft versie 1.5

De in dit Data Pro Statement omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze normale kanalen.

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

Officelynq voor kantoren met gedeelde werkplekken (App, Management Portal, SMART-sensornetwerk).

### 4. Omschrijving product/dienst Officelynq

Officelynq is ontworpen voor gebruikers en verantwoordelijken van kantoren waarin werkplekken en/of vergaderruimten gedeeld worden. Het bestaat uit onderstaande software - en hardware componenten:

- Officelynq App helpt met handige toepassingen zoals het snel en gemakkelijk vinden van collega's en het vinden en indien van toepassing boeken van werkplekken en spreekkamers
- Officelynq Management Portal geeft de gebouw exploitant managementinfo voor gebouw-/faciliteitoptimalisatie, en geeft beheermogelijkheden van het product (gebruikers, faciliteiten, sensoren, instellingen, etc.)
- Officelynq SMART-sensoren en gateways verschaffen i.c.m. Officelynq App de data waarmee bovenstaande functionaliteit geboden wordt.

Zie [www.officelynq.com](http://www.officelynq.com) voor meer informatie.

### 5. Beoogd gebruik

**Product/dienst Officelynq is ontworpen en ingericht om er de volgende soort persoonlijke gegevens van app gebruikers mee te verwerken:**

Naam, functie, afdeling, telefoonnummer, persoonlijke tekst (wordt door gebruiker zelf ingevuld en is niet bedoeld voor bijzondere persoonsgegevens), email adres, profielfoto, gebruikersvoorkeuren, collega's waar men graag bij zit, te vermijden collega's, actuele gebruikers locatie (indien in gebouw met Officelynq sensoren), boekingen van werkplekken of spreekkamers, lopende claim op werkplek of spreekkamer, besturingssysteem smartphone en versie, zoekhistorie (verleden is geanonimiseerd). Zie voor meer informatie [Privacy Statement Officelynq](#). Hierin handelen wij o.a. namens Verwerkingsverantwoordelijke de privacy informatie af naar de gebruikers van de Officelynq Applicaties.

Bij dit product/deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door Opdrachtgever is ter eigen beoordeling door Opdrachtgever.

**6. Data Processor heeft bij het ontwerpen van het product/de dienst *privacy by design* op de volgende wijze toegepast:**

- Opdrachtgevers (gebruikers Management Portal) uploaden zelf de basis persoonlijke gegevens van de beoogde gebruikers en kunnen deze gegevens zelf wijzigen en/of verwijderen. Data Processor controleert de gegevens niet en zal gegevens alleen inzien op verzoek van Opdrachtgever, bijvoorbeeld als dat nodig is om een vraag aan de helpdesk te beantwoorden.
- Gebruikers Officelynq app kunnen zelf persoonlijke informatie aanmaken en verwijderen en instellingen en voorkeuren beheren.
- Dataminimalisatie is toegepast, anonimiseren toegepast op locatiegegevens uit het verleden en zoekhistorie.

**7. Data Processor gebruikt de Data Pro Standaardclausules voor verwerkingen, welke in deel 2, onderaan dit document te vinden zijn.**

**8. Data Processor verwerkt de persoonsgegevens van zijn Opdrachtgevers binnen de EU/EER.**

Dit geldt voor alle als Data Processor verwerkte persoonsgegevens, behalve voor die welke Opdrachtgever zelf naar Data Processor verkiest te versturen per email, zoals bijvoorbeeld voor een support verzoek met persoonsgegevens via email en niet via de supportkanalen van de Officelynq Management Portal.

**9. Indien gegevens buiten de EU/EER verwerkt worden: de Data processor heeft op de volgende manier geborgd dat een passend beschermingsniveau van toepassing is:**

- De organisatie heeft zich aangesloten bij Privacy Shield (Is alleen van toepassing op Microsoft Office 365 en data storage hosting, zie ook punt 10).

## 10. Data Processor maakt gebruik van de volgende sub-processors:

Officelynq's sub Data Processors					
Date: 09-11-2018					
Supplier name	Kind of data	Location of data processing	Relevant certification	Supplier statement	Comment
Microsoft (Office 365)	Office IT Officelynq: Business email, general business data storage and access control/security	Primary in EU	ISO27001	Disclosed upon customer request	Could also be processed outside EU, but Microsoft complies with EU-U.S. Privacy Shield.
Microsoft (Azure)	Production environment incl. customer data storage hosting and access control/security	Primary in EU	ISO27001	Disclosed upon customer request	Could also be processed outside EU, but Microsoft complies with EU-U.S. Privacy Shield.
Microsoft (Azure)	Safe and secure customer data transmissions via VPN	in EU	ISO27001	Disclosed upon customer request	

## 11. Data Processor ondersteunt klanten op de volgende manier bij verzoeken van betrokkenen:

- Gebruikers van Officelynq Management Portal kunnen namens Opdrachtgever zelf basis persoonlijke gegevens van app gebruikers toevoegen, inzien, corrigeren en verwijderen. Daarnaast kunnen ze vanaf nader te benoemen datum, zelfstandig de data uit het webportaal porteren naar een uitvoerbestand. Tot die tijd kunnen verzoeken tot data porteren gericht worden aan ondergenoemde email adres. Hun eigen gegevens kunnen ze als gebruiker van de app behandelen, zoals hieronder beschreven. Voor het opheffen van hun Management Portal gebruikersaccount, kunnen ze een 2<sup>de</sup> lijn support verzoek doen via de supportpagina van de Management Portal.
- Gebruikers van Officelynq app kunnen hun basis persoonlijke gegevens inzien in de app, en laten wijzigen/verwijderen via een verzoek aan de vertegenwoordiger van Opdrachtgever (gebruiker van de Management Portal). Hun overige persoonlijke gegevens kunnen app gebruikers zelf toevoegen, inzien, corrigeren en verwijderen in de app. App gebruikers kunnen een verzoek om hun persoonlijke data te porteren indienen bij onderstaande adres.
- Adres voor verzoeken data porteren: [security@officelynq.com](mailto:security@officelynq.com).

## 12. Na beëindiging van de Overeenkomst met een Opdrachtgever verwijdert Data Processor de persoonsgegevens die hij voor Opdrachtgever verwerkt in principe binnen 2 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).

## 13. Na beëindiging van de Overeenkomst met Opdrachtgever retourneert Data Processor alle persoonsgegevens die hij voor Opdrachtgever verwerkt binnen 3 maanden op de volgende manier:

Opdrachtgever kan vanaf nader te benoemen datum zelfstandig via Officelynq Management Portal, zelf een export (laten) doen (voor die datum kan om de data verzocht worden via [security@officelynq.com](mailto:security@officelynq.com)). Deze exportmogelijkheid wordt gedurende 2 weken na beëindiging

van de Overeenkomst kosteloos geboden. Daarna worden de gegevens verwijderd. Opdrachtgever is zelf verantwoordelijk om voor het tijdstip waarop de Overeenkomst eindigt afspraken te maken over een eventuele andere manier of een andere tijdstip van het retourneren van de data. Afhankelijk van de wensen kunnen hier kosten voor in rekening gebracht worden.

## BEVEILIGINGSBELEID

### 14. Data Processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:

- Data Processor heeft beveiligingsbeleid voor vertrouwelijkheid, integriteit en beschikbaarheid van data van Opdrachtgevers, waaronder persoonlijke gegevens van berokken Data subjects opgesteld; dit wordt periodiek: gecommuniceerd, gecontroleerd en geactualiseerd/verbeterd;
- Personeel en ingehuurde professionals die in aanraking kunnen komen met persoonsgegevens van betrokkenen of andere vertrouwelijke gegevens van Opdrachtgever, zijn daarvoor opgeleid en/of geïnstrueerd en hebben allen een geheimhoudingsverklaring getekend;
- Alle ingeschakelde sub Data Processors worden zorgvuldig beoordeeld voordat ze gecontracteerd worden, daarna blijven ze periodiek beoordeeld worden en alleen ingezet zolang ze aan de gestelde eisen blijven voldoen;
- Gezien de aard van de gebruikte data (zie punt 5) en het overwegend open karakter daarvan, is alleen gekozen om de locatiegegevens van gebruikers van de Officelynq app in het verleden, compleet te anonimiseren; Dat betekent dat ze niet meer tot de persoon herleidbaar zijn; Pseudonimiseren van de overige gegevens zou te veel gebruikersongemak opleveren bij het wisselen het mobiele apparaat waarop gebruiker Officelynq app gebruik, en staat daarmee niet in verhouding tot de voordelen op privacy gebied.
- Om te borgen dat bij een incident de beschikbaarheid van en de toegang tot de (persoons)gegevens tijdig hersteld wordt, is er een procedure met zowel technische als organisatorische maatregelen van kracht: IS continuity plan Officelynq;
- De technische maatregelen die zijn genomen om de data van Opdrachtgever, waaronder de persoonsgegevens van betrokken Data subjects veilig, vertrouwelijk en beschikbaar te houden zijn:
  - De data wordt per Opdrachtgever gescheiden opgeslagen op aparte virtuele servers;
  - De data wordt voor elke Opdrachtgever opgeslagen op servers die zijn ondergebracht in een daartoe uitgerust datacenter, met ISO27001 certificering, waarvan de Statement of Applicability voldoende beoordeeld is, met een gegarandeerde hoge beschikbaarheid;
  - De data wordt periodiek en geautomatiseerd in backups opgeslagen;
  - De beheerconsole van de servers waar de data op staat, is alleen bereikbaar via een speciale VPN-verbinding en de toegang tot die beheersconsole is uitgerust met Multi-Factor Authentication (MFA);
  - Communicatie tussen de servers met persoonsgegevens en Officelynq App/Management Portal, is beveiligd met SSL-certificaten;

- Communicatie tussen de servers met de persoonsgegevens en andere servers gaat altijd via een beveiligde VPN-verbinding.

**15. Data Processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**

- ISO 27001.

**DATALEKPROTOCOL**

**16. In geval er toch iets mis gaat, hanteert Data Processor het volgende datalekprotocol om ervoor te zorgen dat klanten op de hoogte zijn van incidenten:**

- Data Processor zal zich inspannen de hieronder nader uitgewerkte beveiligingsincidenten zonder onredelijke vertraging te melden aan Opdrachtgever: onwettelijke verwerking, vernietiging, verlies, wijziging, ongeoorloofde verstrekking van en ongeoorloofde toegang tot persoonsgegevens van Opdrachtgever en haar betrokken Data subjects;
- Data Processor heeft in het kader van het melden van beveiligingsincidenten de volgende maatregelen getroffen:
  - Personeel van Data Processor en haar leveranciers/onderaannemers melden beveiligingsincidenten aan de Security Officer van Data Processor.
  - Deze stelt vast of er inderdaad sprake is van een beveiligingsincident en bepaalt ook de aard (o.a. of het ook om persoonsgegevens gaat), ernst, omvang, betreft stakeholders, bepaalt met hen vervolgstappen, eerst t.b.v. stoppen datalek en dan de stappen daarna, bewaakt deze en zorgt voor registratie.
  - E.e.a. is vastgelegd in de procedure 'Incident and data leak management Officelynq', welke Opdrachtgever op verzoek in kan zien.
- Data Processor zal bij het doen van zijn melding aan Opdrachtgever de volgende afspraken in acht nemen:
  - De melding wordt gedaan per email naar een door Opdrachtgever, bij opdracht te verstrekken email-adres, met als onderwerp 'Security Incident'.
  - De contactpersoon van Data Processor voor beveiligingsincidenten is:
    - Naam: Quanjing Li;
    - Email: security@officelynq.com
    - Telefoon: +31615285737
  - De melding zal bestaan uit het model meldingsformulier van de Autoriteit Persoonsgegevens (<https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?0>), ingevuld voor zover mogelijk op het moment van indienen. Zo nodig en gewenst volgen updates met steeds geactualiseerde informatie.
  - Data Processor is gerechtigd om op verzoek van Opdrachtgever uitgevoerde extra werkzaamheden, t.a.v. bijvoorbeeld informatieverstrekking of vervolgacties t.b.v. voorkoming en/of reparatie van het beveiligingsincident, in rekening te brengen bij Opdrachtgever, tegen de in de Overeenkomst afgesproken uurtarieven.
  - Data Processor zal datalekken niet zelfstandig melden bij AP, daar dit ter beoordeling van en voor verantwoordelijkheid van Opdrachtgever is.

# DEEL 2: STANDAARDCLAUSULES

## VOOR VERWERKINGEN

*versie: januari 2018*

*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):** toezichhoudende 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, subverwerkers, 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, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van 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.
- 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 inaccessible*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen 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 kan de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige.
- 7.4 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.
- 7.5 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.
- 7.6 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. SUBVERWERKERS**

- 8.1 Data Processor heeft in het Data Pro Statement vermeldt of, en zo ja welke derde partijen (subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.
- 8.2 Opdrachtgever geeft toestemming aan Data Processor om andere subverwerkers 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.