
# STANDAARD VERWERKERS-OVEREENKOMST

*Lucas IT B.V.*

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Editie januari 2018

Versie 1.0

# DEEL 1: DATA PRO STATEMENT

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

## ALGEMENE INFORMATIE

**1. Dit Data Pro Statement is opgesteld door:**

Lucas IT B.V. gevestigd en kantoorhoudend te 7665 SH Albergen aan de Zandhuisweg 1, KvK: 06091413.
Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden via:
privacy@lucasit.nl en/of 0546-442322

**2. Dit Data Pro Statement geldt vanaf 22-5-2018 en betreft versie 1.0**

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 diensten van data processor**

A. **Proactieve Monitoring**
B. **Support**
C. **Beheer & Onderhoud**
D. **Antivirus**
E. **Firewall**
F. **Anti-spam & ATP**
G. **E-mail**
H. **Cloud storage**
I. **Hosted werkplek**
J. **Office 365 & Azure**
K. **Google Apps**
L. **Webhosting**
M. **Voip**
N. **Back-up**
O. **Colocatie**
P. **Internetdiensten**

**4. Omschrijving diensten**

A. **Monitoring**
   24x7 Monitoren van de systeemprocessen en controle IT omgeving middels digitale hartbewaking.
B. **Support**
   Ondersteuning op afstand en terplekke voor de IT omgeving.
C. **Beheer & Onderhoud**
   Onderhoud en beheer IT-omgeving en IT-componenten.
D. **Antivirus**
   Bescherming IT-omgeving IT-componenten on-premise of cloud antivirus.
E. **Firewall**
   Poortwachter van netwerk om inkomend en uitgaand verkeer te monitoren en beveiligen.
F. **Anti-spam & ATP**
   Cloud diensten om de mail en/of surfverkeer op te schonen en te beveiligen.
G. **E-mail**
   E-mail Server vanuit de Cloud, voor o.a. mail, agenda, adresboek en taken.

H. **Cloudstorage**
Cloud dienst voor opslag bestanden, zoals o.a. tekstbestanden, fotobestanden, videobestanden, audiobestanden en archiefbestanden

I. **Hosted werkplek**
Online werkplek in de Cloud.

J. **Office 365/Azure**
Cloud diensten van Microsoft voor Online werken.

K. **Google Apps**
Cloud diensten van Google voor Online werken.

L. **Webhosting**
Domeinregistratie, mail forwarding en webruimte voor zakelijke hosting. Geen onderhoud aan de website zelf.

M. **Voip**
Bellen via de Cloud via SIP of Online telefooncentrale.

N. **Back-up**
Reserve kopie van gegevens naar offsite of online locatie.

O. **Colocatie**
Klant apparatuur of Private of Public Cloud diensten vanuit datacenter geserveerd.

P. **Internetdiensten**
Infra voor uw IT omgeving om data te versturen/ontvangen van A naar B.

**5. Beoogd gebruik**

**De diensten uit punt 3 zijn ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:** E-mailberichten, Agenda afspraken, contactpersonen, mailgegevens, tekstbestanden, fotobestanden, videobestanden, audiobestanden en archiefbestanden.

**Bij deze diensten is niet rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten mee te verwerken. Verwerken van deze gegevens met het hiervoor omschreven dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.**

**6. Data processor gebruikt de Data Pro Standaardclausules voor eigen verwerkersovereenkomst, welke op https://www.lucasit.nl/avg te vinden zijn.**

**7. Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers binnen en buiten de EU/EER.**

**8. Data processor maakt gebruik van de volgende sub-processors:**
Ten behoeve van de veiligheid van onze diensten, de privacy van onze klanten en concurrentiegevoelige informatie, zijn onze sub-processors geanonimiseerd. Indien u als opdrachtgever inzage wilt hebben in de sub-processors voor de diensten die u bij ons afneemt, kunt u telefonisch contact opnemen via 0546-442322, of per e-mail via privacy@lucasit.nl. De data-processor kan hier kosten voor inrekening brengen.

- **Microsoft (binnen EU/EER)**

De gegevens die via Microsoft worden verwerkt, worden verwerkt binnen de Europese Unie.

- **Twin datacenter (binnen EU/EER)**

De meeste van onze eigen clouddiensten staan in een Twin datacenter in Overijssel Nederland. De data welke wordt verwerkt in dit datacenter, blijft in Overijssel.

- **AntiSpam SAAS (binnen EU/EER)**

Gegevens kunnen verwerkt worden door onze sub-verwerkers Antispam SAAS. Deze partijen verwerken data binnen de EU/EER.

- **Nieuwsbriefsysteem (buiten EU/EER)**

De nieuwsbrieven van Lucas IT worden door onze sub-verwerker Nieuwsbriefsysteem verwerkt. Dit systeem verwerkt data in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert het nieuwsbriefsysteem zich aan het EU-U.S. Privacy Shield.

- **Internetproviders (binnen EU/EER)**

Internetdiensten in Cogas, Ziggo, KPN en Caiway gebied.

- **Centrale handtekening software (binnen EU/EER)**

Handtekeningensoftware gesitueerd binnen EER

- **Dedicated WordPress en Woocommerce hosting (binnen EU/EER)**

Zakelijke webhosting gesitueerd binnen EU/EER en Nederland.

- **Professional Service Automation (buiten EU/EER)**

Deze online diensten worden door onze sub-verwerker PSA systeem verwerkt. Dit systeem verwerkt data o.a. in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert het PSA zich aan BCR (Binding Corporate Rules.

- **Online hulpdienst (buiten EU/EER)**

Online hulpmiddel voor live ondersteunen van klanten.

- **Google (buiten EU/EER)**

Deze online diensten worden door onze sub-verwerker Google verwerkt. Dit systeem verwerkt data o.a. in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert Google zich aan het EU-U.S. Privacy Shield.

- **Cloud Antivirus (binnen EU/EER)**

Cloud Antivirus binnen EER.

- **Endpoint Management en Remote Monitoring Systeem (buiten EU/EER)**

Deze online diensten worden door onze sub-verwerker Endpoint Management en Remote Monitoring Systeem verwerkt. Dit systeem verwerkt data o.a. in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert het Endpoint Management en Remote Monitoring Systeem zich aan het EU-U.S. Privacy Shield.

9. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**

De opdrachtgever kan een verzoek van ondersteuning bij, inzageverzoeken, correctieverzoeken, verwijderingsverzoeken en dataportabiliteitsverzoeken van een betrokkene aan de opdrachtgever, per e-mail via privacy@lucasit.nl kenbaar maken aan de data processor. De opdrachtgever moet de data processor van informatie voorzien over: de betrokkene, het soort verzoek en de betrokken systemen, databases en diensten. De data processor maakt een besluit over de goedkeuring van het verzoek, waarop vervolgens het contactpersoon van de opdrachtgever per e-mail wordt ingelicht over het besluit, ingeval negatief met onderbouwing van het besluit, en de mogelijke vervolgstappen van ondersteuning mits van toepassing. Lees meer in artikel 7.1.

10. **Na beëindiging van de overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen drie maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**

De gegevens worden veelvoudig overschreven door middel van het overschrijven met nieuwe data.

11. **Na beëindiging van de overeenkomst met opdrachtgever kan de data processor op verzoek, alle persoonsgegevens die hij voor opdrachtgever verwerkt, binnen 4 weken op de volgende manier retourneren:**

Indien de betreffende dienst dit toelaat, kan de opdrachtgever zelf via de dienst een export maken. De exportmogelijkheid is beschikbaar tot 4 weken na beëindiging van de overeenkomst. Daarna worden de gegevens verwijderd. Op verzoek worden de gegevens via een gegevensdrager persoonlijk overhandigd in het formaat zip-archief. Er worden voor het op verzoek overhandigen van gegevens wel kosten in rekening gebracht. De kosten die in rekening worden gebracht bij een verzoek tot overhandigen van de gegevens zijn de kosten van de gegevensdrager, verzending en de te verrichten handelingen.

## BEVEILIGINGSBELEID

**12. Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn dienst(en):**

- het naleven van de in artikel 5 van de Data Pro Standaardclausules voor verwerkingen genoemde geheimhoudingsverplichting;
- de medewerkers, welke werken met persoonsgegevens, hebben in een ondertekend arbeidsovereenkomst een geheimhoudingsverklaring staan en aanvullende gedragsregels in een separate arbeidsvoorwaarden regelement;
- het toepassen van encryptie op opslag van gevoelige gegevens (indien van toepassing en gevraagd);
- het hanteren van een patchmanagement t.b.v. het up-to-date houden van servers, netwerkapparatuur desktops en mobiele apparaten (indien van toepassing en gevraagd);
- het hanteren van een role & access management, waardoor alleen de door de data-processor toegewezen personen toegang hebben tot gevoelige gegevens;
- Administrator/beheer-accounts, mogen alleen op verzoek van klant worden verstrekt vanuit directie/management data-processor, aan directie/management eindklant;
- het inzetten van intern gescheiden netwerken d.m.v. VLAN's of DMZ;
- het inzetten van, en het onderhouden softwarematige beveiliging (antivirus, anti-ransomware, firewall, enz) en fysieke IT-beveiligingssystemen (next-generation firewalls);
- het trainen van medewerkers op informatiebeveiligingsbewustzijn;
- intern heeft de data-processor camerabewaking, sleutelbeheer, beweegmelders en alarmsysteem met certificering toegepast;
- intern hanteert de data-processor individuele gebruikersnamen, wachtwoorden en meerfactorauthenticatie, met passend wachtwoordbeleid, veilige VPN-tunnels en encryptie van externe datasystemen. Toegang tot systemen wordt gelogd;
- documenten met gevoelige informatie worden vernietigd door een professionele archief vernietiger;
- de data-processor doet vooraf een selectie op basis van eigen onderzoek naar sub-data-processor;
- de data-processor heeft (indien van toepassing en gevraagd) het productiesysteem gescheiden van het ontwikkel- test- en acceptatiesysteem;
- op speciaal verzoek en tegen additionele kosten kan de klant gebruik maken van een gecertificeerde 'data erase' dienst.

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

- De data-processor stelt ISO 27001 en NEN7510 als leidraad voor de IT-dienstverlening.
- Het datacenter welke Lucas IT gebruikt voor haar diensten past de volgende ISMS toe: ISO 27001, ISO 9001, ISO 14001 en NEN 7510.
- Microsoft past op haar datacenter de volgende ISMS toe: ISO 27001, ISO 27018 en FedRAMP.

**14. Data processor heeft de volgende certificeringen**

- Op de roadmap van de data-processor staat de certificering voor ISO 27001 en NEN 7510.

## DATALEKPROTOCOL

**15. In geval er toch iets mis gaat, hanteert data processor het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**

De data processor gebruikt monitoringtools om potentiele beveiligingsincidenten te signaleren. Indien u als opdrachtgever inzage wilt hebben in de monitoringtools voor de diensten die u bij ons afneemt, kunt u telefonisch contact opnemen via 0546-442322, of per e-mail via privacy@lucasit.nl.

Door het gebruik van deze monitoringtools, worden alle systemen (hardware, software, cloud) gekoppeld aan één centrale monitoringomgeving. De monitoringtool verwerkt de output van deze systemen automatisch op basis van vooraf vastgestelde filters en eigenschappen, waarna de monitoringtool een melding geeft van alerts.

Er is een procedure voor het intern melden van incidenten. Indien de data processor in zijn organisatie of de organisatie van de controller een datalek ontdekt, zal de data processor zijn opdrachtgever daarvan zo snel mogelijk op de hoogte stellen, door contact op te nemen met de contactpersoon van de opdrachtgever, door een email te sturen vanaf privacy@lucasit.nl aan dit contactpersoon . De data processor levert zo veel (indien) mogelijk relevante gegevens aan, waaronder:

- de omschrijving van het incident;
- de aard van de inbreuk;
- aard van (categorieën) persoonsgegevens van betrokkenen;
- schatting van het aantal betrokken data subjects;
- de mogelijk betrokken databases;
- indicatie wanneer het incident heeft plaatsgevonden;
- contactgegevens contactpersoon (FG) (waar kan de controller met vragen terecht?);
- Mogelijke gevolgen (wat kan er gebeuren, waar moet controller dan wel data subject op bedacht zijn, wijzen op mogelijkheden identiteitsfraude als gegevens als BSN nummers, inlog en wachtwoordgegevens, paspoort kopieën etc. in verkeerde handen terecht zijn gekomen);
- Genomen maatregelen (wat heeft de data processor gedaan om eventuele schade te beperken of dit in de toekomst te voorkomen?); en
- Te nemen maatregelen door de controller dan wel betrokken data subjects (wat kunnen betrokken data subjects zelf doen, bijvoorbeeld “houd mail in de gaten, wijzig wachtwoorden”).

Meldingen van incidenten worden indien mogelijk binnen 24 uur gedaan aan de opdrachtgever. De data processor zal zelf geen melding doen aan de AP of data subjects. Het wel of niet melden blijft de verantwoordelijkheid van de controller. De data processor zal de opdrachtgever of de controller desgewenst ondersteunen bij het meldingsproces.

# 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. **Autoriteit Persoonsgegevens (AP):** toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 Avg.
2. **Avg:** de Algemene verordening gegevensbescherming.
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.
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.
5. **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon.
6. **Opdrachtgever:** partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.
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.
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.
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

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. 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.
3. Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.
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.

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.
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.
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.
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

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.
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. 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.
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.
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.
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

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.
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.
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. 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

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

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

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.
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.
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.
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.
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.
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.