# STANDAARD VERWERKERS-OVEREENKOMST

*Lucas IT B.V.*

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Editie oktober 2026

Versie 1.5

# 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 AA Albergen aan de Philippus Robbenstraat 9A, 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 1.5**

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 diensten van verwerker**

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. **Microsoft 365 Copilot & Azure**
K. **Google Apps**
L. **Webhosting**
M. **Voip**
N. **Back-up**
O. **Colocatie**
P. **Internetdiensten**
Q. **Hosted Bureaublad**
R. **VPS**
S. **MDR**
T. **Security Awareness**
U. **Centrale Management Systemen**
V. **Dark Web Monitoring**
W. **MFA**
X. **SaaS Monitoring**
Y. **Geautomatiseerde Pentest**
Z. **Professional Service Automation tool**
AA. **Nieuwsbrievensysteem**
BB. **Centrale handtekening software**
CC. **Internetdiensten**
DD. **Credentials Management Systeem**
EE. **Wachtwoordenkluis**
FF. **Managed Wi-Fi controller**
GG. **Safe Relay**

**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. Microsoft 365 Copilot /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, offline of online locatie. Voor zover dit expliciet in de dienstverlening of overeenkomst is aangegeven, kan deze dienst worden gebruikt voor het verwerken van bijzondere persoonsgegevens.

**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.

**Q. Hosted Bureaublad**

Online bureaublad met applicaties in de Cloud.

**R. VPS**

Een Virtual Private (web)Server (VPS) in de Cloud.

**S. MDR**

24/7 beveiligingsmonitoring, geavanceerde preventie, detectie en mitigatie van cyberdreigingen, plus gerichte, risicogebaseerde thread hunting door een Managed SOC.

**T. Security Awareness**

Om datalekken te voorkomen biedt deze dienst een e-learning programma voor medewerkers en phishing simulaties.

**U. Centrale Management Systemen**

Voor het Centraal beheren van NAS-systemen, firewalls en Acces points.

**V. Dark Web Monitoring**

24/7 monitoring door mens en machine van het dark web of er credentials zijn gelekt.

**W. MFA**

Diensten voor het inloggen met MFA.

X. **SaaS Monitoring**
Met behulp van machine learning afwijkingen in gebruikersgedrag detecteren in SaaS applicaties.

Y. **Geautomatiseerde Pentest**
Het automatisch detecteren van kwetsbaarheden in het netwerk, zowel van buitenaf als van binnen.

Z. **Professional Service Automation tool**
Lucas IT gebruikt een PSA systeem voor o.a. CRM, Projectmanagement, Servicedesk en SLA management.

AA. **Nieuwsbrievensysteem**
Voor het versturen van nieuwsbrieven.

BB. **Centrale handtekening software**
Handtekeningensoftware t.b.v. e-mailhandtekeningen

CC. **Internetdiensten**
Internetdiensten in Cogas, Ziggo, KPN en Caiway gebied.

DD. **Credentials Management Systeem**
Voor veilige opslag van credentials, apparaat- en/of netwerkinformatie door Lucas IT

EE. **Wachtwoordenkluis**
Eigen online kluis om wachtwoorden in op te slaan.

FF. **Managed Wi-Fi controller**
Voor het centraal beheren van Wi-Fi acces points

GG. **Safe Relay**
Het veilig mailen voor zorgklanten. Deze dienst is geschikt voor het verwerken van bijzondere persoonsgegevens.

**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, tenzij expliciet anders aangegeven. Verwerken van deze gegevens met het hiervoor omschreven dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.**

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

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

**8. Verwerker maakt gebruik van de volgende sub-verwerkers:**
Ten behoeve van de veiligheid van onze diensten, de privacy van onze klanten en concurrentiegevoelige informatie, zijn onze sub-verwerkers geanonimiseerd. Indien u als opdrachtgever inzage wilt hebben in de sub-verwerkers 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 verwerker kan hier kosten voor inrekening brengen.

- **Microsoft (binnen EU/EER)**
  Lucas IT gebruikt deze sub-verwerker o.a. voor het aanbieden van Microsoft clouddiensten. 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. Het datacenter is gecertificeerd voor ISO 27001:2022, ISO 27017, ISO 27018, ISO 9001:2015, ISO 14001:2015 en NEN 7510:2017. Tevens beschikt het over een SOC2 verklaring.
- **AntiSpam & ATP SAAS (binnen EU/EER)**
  Gegevens kunnen verwerkt worden door onze sub-verwerkers Antispam & ATP 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. Deze sub-verwerker 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.
- **Breedbandnetwerk in Nederland en Duitsland (binnen EU/EER)**
  Internetdiensten ten behoeve van zakelijke connectiviteit. Deze partij is gevestigd in Nederland.
- **Centrale handtekening software (binnen EU/EER)**
  Handtekeningensoftware t.b.v. e-mailhandtekeningen is gesitueerd binnen EU.
- **Professional Service Automation tool (buiten EU/EER)**
  Lucas IT gebruikt een PSA systeem voor o.a. CRM, Projectmanagement, Servicedesk en SLA management. Deze sub-verwerker 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 en het EU-U.S. Privacy Shield.
- **Online hulpdienst (binnen EU/EER)**
  Online hulpmiddel voor live ondersteunen (remote support) van klanten. De sub-verwerker is gevestigd in Duitsland.
- **Google (buiten EU/EER)**
  Deze sub-verwerker 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)**
  Lucas IT gebruikt t.b.v. antivirusbescherming en Cloud Antivirus dienst een sub-verwerker Cloud Antivirus binnen EU.
- **Endpoint Management en Remote Monitoring Systeem (buiten EU/EER)**
  Lucas IT gebruikt t.b.v. monitoring van endpoints een sub-verwerker voor Endpoint Management en Remote Monitoring Systeem (RMM). Deze sub-verwerker 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.
- **Credentials Management Systeem (buiten EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor veilige opslag van credentials, apparaat- en/of netwerkinformatie. Deze sub-verwerker verwerkt data in Canada. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert het Credentials Management Systeem zich aan het SOC2.
- **Hosted werkplek (binnen EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van een hosted werkplek in de Cloud. De sub-verwerker is gevestigd in Nederland.
- **Cloud Hosting Platform Manager (binnen EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van Virtual Private Servers (VPS). Deze sub-verwerker houdt kantoor binnen de Europese Unie (EU) en verwerkt data van cloud oplossingen in Amsterdam (AMS).
- **Cloud Hosting Platform en Domein registratieservice (binnen EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van webhosting en domeinregistratie. Deze sub-verwerker verwerkt data van oplossingen in Amsterdam (AMS). De sub-verwerker is gevestigd in Nederland.
- **Managed SOC (Binnen EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van MDR. Een sub-verwerker binnen EU.
- **Security Awareness (buiten EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van e-learning en phishing simulaties. Deze sub-verwerker verwerkt data o.a. in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert Security Awareness zich aan BCR (Binding Corporate Rules en het EU-U.S. Privacy Shield.
- **Dark Web Monitoring (buiten EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van Dark web monitoring Deze sub-verwerker verwerkt data o.a. in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert Dark Web Monitoring zich aan BCR (Binding Corporate Rules en het EU-U.S. Privacy Shield.
- **SaaS Monitoring (buiten EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van SaaS Monitoring. Deze sub-verwerker verwerkt data o.a. in de

Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert Dark Web Monitoring zich aan BCR (Binding Corporate Rules en het EU-U.S. Privacy Shield.

- **Geautomatiseerde Pentest (buiten EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van een Geautomatiseerde Pentest. Deze sub-verwerker verwerkt data o.a. in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert Geautomatiseerde Pentest zich aan BCR (Binding Corporate Rules en het EU-U.S. Privacy Shield.
- **Managed Wi-Fi controller (buiten EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van Managed Wi-Fi controller. Deze sub-verwerker verwerkt data o.a. in de Verenigde Staten. Om het Europese veiligheid en privacy niveau te waarborgen, conformeert Managed Wi-Fi controller zich aan BCR (Binding Corporate Rules en het EU-U.S. Privacy Shield.
- **Safe Relay (Binnen EU/EER)**
  Lucas IT gebruikt deze sub-verwerker voor het aanbieden van Safe Relay. Een sub-verwerker binnen EU.

**9. Verwerker 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 verwerker. De opdrachtgever moet de verwerker van informatie voorzien over: de betrokkene, het soort verzoek en de betrokken systemen, databases en diensten. De verwerker 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 verwerker 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 op een veilige manier digitaal overgedragen in een geschikt formaat of 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. Verwerker 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 verwerker toegewezen personen toegang hebben tot gevoelige gegevens;
- Administrator/beheer-accounts, mogen alleen op verzoek van klant worden verstrekt vanuit directie/management verwerker, 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 verwerker camerabewaking, sleutelbeheer, beweegmelders en alarmsysteem met certificering toegepast;
- intern hanteert de verwerker 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 verwerker doet vooraf een selectie op basis van eigen onderzoek naar sub-verwerker;
- de verwerker 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. Verwerker heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**

- De verwerker 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 27001:2022, ISO 27017, ISO 27018, ISO 9001:2015, ISO 14001:2015 en NEN 7510:2017. Tevens een SOC2 verklaring.
- Microsoft past op haar datacenter de volgende ISMS toe: ISO 27001:2022, ISO 27017:2015, ISO 27018:2019, ISO 27701:2019, ISO 22301:2019 en FedRAMP.
- De verwerker conformeert zich bij gegevensuitwisseling met zorgverleners aan de eisen en beheersmaatregelen zoals vastgelegd in de NEN 7512:2022.
- De verwerker conformeert zich bij het vastleggen, beheren en beveiligen van logging op persoonlijke gezondheidsinformatie aan de eisen en beheersmaatregelen zoals vastgelegd in de NEN 7513:2024.

**14. Verwerker heeft de volgende certificeringen**

- De verwerker is gecertificeerd conform ISO 27001:2022 en NEN 7510:2024.

## DATALEKPROTOCOL

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

De verwerker gebruikt monitoringtools om potentiële 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 verwerker in zijn organisatie of de organisatie van de verwerkingsverantwoordelijke een datalek ontdekt, zal de verwerker 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 verwerker 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 verwerkingsverantwoordelijke met vragen terecht?);
- Mogelijke gevolgen (wat kan er gebeuren, waar moet verwerkingsverantwoordelijke 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 verwerker gedaan om eventuele schade te beperken of dit in de toekomst te voorkomen?); en
- Te nemen maatregelen door de verwerkingsverantwoordelijke 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 verwerker zal zelf geen melding doen aan de AP of data subjects. Het wel of niet melden blijft de verantwoordelijkheid van de verwerkingsverantwoordelijke. De verwerker zal de opdrachtgever of de verwerkingsverantwoordelijke desgewenst ondersteunen bij het meldingsproces.

# DEEL 2: STANDAARDCLAUSULES VOOR VERWERKINGEN

**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 **Verwerker**: 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 Verwerker waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, sub-verwerkers, 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 de Verwerker persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke zijn als een andere verwerker.

1.7 **Overeenkomst**: de tussen Opdrachtgever en Verwerker 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 Verwerker 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 Verwerker 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 Verwerker 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 Verwerker worden aangepast aan veranderende omstandigheden. Verwerker 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 Verwerker verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Verwerker 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 Verwerker 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 Verwerker 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 Verwerker 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 Verwerker 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 Verwerker, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Verwerker.

## ARTIKEL 3. BEVEILIGING

3.1 Verwerker treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Verwerker 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 Verwerker 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 Verwerker streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Verwerker 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 Verwerker kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Verwerker 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 Verwerker verzoeken nadere beveiligingsmaatregelen te treffen. Verwerker is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Verwerker 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 Verwerker de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

## ARTIKEL 4. INBREUKEN IN VERBAND MET PERSOONSGEGEVENS

4.1 Verwerker staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Verwerker 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 Verwerker 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 Verwerker 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). Verwerker is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Verwerker 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 Verwerker 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 Verwerker waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

5.2 Verwerker 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 Verwerker aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Verwerker 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 Verwerker 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 Verwerker 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 Verwerker belet. In een dergelijk geval zal Verwerker de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Verwerker 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 Verwerker 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 Verwerker direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Verwerker 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 Verwerker zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

7.4 Verwerker 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 Verwerker 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 Verwerker heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Verwerker verstrekken. Verwerker 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. Verwerker
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 Verwerker 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 Verwerker heeft in het Data Pro Statement vermeld of, en zo ja welke derde partijen (sub-processors of subverwerkers) Verwerker inschakelt bij de verwerking van de Persoonsgegevens.

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

8.3 Verwerker zal Opdrachtgever informeren over een wijziging in de door de Verwerker ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Verwerker. Verwerker 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 Verwerker 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.