Constant IT

Verwerkersovereenkomst

Versie 1.0

30/7/2018

Deel I – Data Pro Statement

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst.

Algemene informatie

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

   Constant IT B.V.
   Paul van Vlissingenstraat 6c
   1096 BK Amsterdam

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met privacy@constant.it of +31 20 – 760 8700.

2. Dit Data Pro Statement geldt vanaf 25 mei 2018.

   De in dit Data Pro Statement omschreven beveiligingsmaatregelen actualiseert Data Processor regelmatig om ten aanzien van data protectie actueel te blijven. Data Processor houdt u op de hoogte van wijzigingen via haar normale kanalen.

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van Data Processor:
   - Managed Services & Support: een Managed Services overeenkomst en/of het uitvoeren van werkzaamheden op basis van de Constant IT tariefkaart
   - Projects & Consultancy: een opdracht tot uitvoer van een project en/of het uitvoeren van werkzaamheden op basis van de Constant IT tariefkaart

   Dit Data Pro Statement is NIET van toepassing op producten en diensten van derden. Op deze diensten zijn de voorwaarden van toepassing van de desbetreffende leverancier. Deze zijn terug te vinden op de website van de leverancier of op verzoek op te vragen bij Constant IT. Dit geldt onder andere voor cloud diensten welke Constant IT aan haar klanten levert. Hieronder:

   - Microsoft Office 365
   - Microsoft 365
   - Microsoft Azure
   - RoutIT HIP
   - KPN EEN
   - RoutIT internetverbinding
   - Domeinnaamregistratie en hosting
   - StoreGrid, Acronis en Altaro back-up

4. Beoogd gebruik van de producten en diensten vermeld onder punt 3 gaat de Data Processor niet na welke (persoons) gegevens verwerkt worden. Meer in algemene zin kan het daarbij gaan om verwerking van (persoons) gegevens in e-mailberichten, agenda afspraken, contactpersonen, tekstbestanden, databestanden en datadragers. De (persoons) gegevens zal Data Processor uitsluitend verwerken in het kader van de Overeenkomst conform de instructies van Opdrachtgever en in overeenstemming met de Opdrachtgever bepaalde doeleinden en middelen. Data Processor verwerkt Persoonsgegevens niet anders dan in de Overeenkomst voorzien. Met name gebruikt de Data Processor de (persoons) gegevens niet voor eigen doeleinden.

   Bij de producten en diensten is verder 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 product of dienst door Opdrachtgever is ter eigen beoordeling door Opdrachtgever.

5. Data Processor gebruikt de Data Pro Standaardclausules voor verwerkingen, welke onderdeel zijn van dit document.

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

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

   - Microsoft - verwerkt de persoonsgegevens binnen de EU/EER
   - Autotask - verwerkt de persoonsgegevens binnen de EU/EER
   - Exact - verwerkt de persoonsgegevens binnen de EU/EER
   - IT Glue - verwerkt de persoonsgegevens binnen de EU/EER

8. Data Processor ondersteunt Opdrachtgever op de volgende manier bij verzoeken van betrokkenen: Data Processor zal, voor zover redelijk mogelijk, door middel van technische en organisatorische maatregelen Opdrachtgever ondersteunen bij het vervullen van diens plicht om verzoeken waarbij een betrokkene zijn rechten uitoefent, te beantwoorden. De beslissing of, en zo ja, in hoeverre, Opdrachtgever uitvoering geeft aan een verzoek waarbij een betrokkene zijn rechten uitoefent, blijft volledig bij Opdrachtgever rusten.

   Data Processor zal, op eerste schriftelijke verzoek van Opdrachtgever, zo snel mogelijk maar in ieder geval niet later dan binnen tien (10) werkdagen, overgaan tot:

   - het schriftelijk verstrekken van alle door Opdrachtgever gewenste persoonsgegevens van de betrokkene die het verzoek heeft gedaan tot inzage
   - het schriftelijk verstrekken van alle door Opdrachtgever gewenste Persoonsgegevens van de betrokkene die het verzoek heeft gedaan tot inzage;

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

Indien betrokkene zich direct richt tot Data Processor ter uitoefening van zijn rechten, dan zal Data Processor onverwijld de betrokkene doorverwijzen naar de Opdrachtgever.

9. In beginsel slaat Data Processor geen persoonsgegevens op van een Opdrachtgever op haar eigen systemen. Na beëindiging van de overeenkomst met een Opdrachtgever verwijdert Data Processor dan ook alleen de persoonsgegevens die hij voor Opdrachtgever expliciet opslaat en verwerkt op haar eigen systemen. Dit in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible). Door het gebruik van sub-processors en complexe ICT-systemen kan verwijdering niet worden gegarandeerd. Hieronder ook ontvangen en verzonden e-mails en eventuele bijlages, chatberichten en documenten in de Microsoft cloud, tickets en eventuele bijlages in Autotask en data/bestanden in andere ICT-systemen welke wordt opgeslagen bij (andere) sub-processors en op fysieke en/of virtuele systemen van Constant IT.

Beveiligingsbeleid

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

    Organisatorische maatregelen: organisatorische maatregelen die genomen zijn:

    - Training en bewustzijn van medewerkers
    - Kennis en competentie van medewerkers
    - Procedures en instructies

    Technische maatregelen: technische maatregelen die genomen zijn:

    - Fysieke beveiliging van ruimtes
    - Digitale beveiliging van systemen en applicaties, door middel van:
        - Update en patch routines
        - Antivirus en malware beveiliging
        - Firewalls ter bescherming van netwerk en computers
        - Encryptie van opgeslagen data op computers
        - Logging van dataverkeer
        - Wachtwoordbeheer en beleid voor eigen systemen en systemen van derden
        - Uitgebreide autorisaties voor eigen systeemtoegang

Datalekken

In geval van een (potentieel) datalek, hanteert Data Processor het volgende datalekprotocol om ervoor te zorgen dat Opdrachtgever op de hoogte is van incidenten.

1 Datalekprotocol

1.1 Aanleiding

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat Constant IT verplicht is om (potentiële) datalekken te melden aan de toezichthouder, de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de betrokkene van wie de gegevens zijn gelekt. Als blijkt dat niet of onvoldoende is voldaan aan deze meldplicht kan de toezichthouder een boete opleggen.

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) formeel van kracht die de Wet bescherming persoonsgegevens (Wbp) zal vervangen. Onder de AVG geldt tevens de meldplicht datalekken.

Volgens de AVG is er sprake van een datalek als zich een inbreuk voordoet op de beveiligingsmaatregelen, wat leidt tot het per ongeluk, opzettelijk of onrechtmatig vernietigen, verliezen, aanpassen, ongeautoriseerde openbaring van, of toegang tot, persoonsgegevens die overgedragen, bewaard of op een andere manier verwerkt zijn. Voorbeelden van een datalek zijn het verlies of diefstal van een mobiel apparaat, waaronder laptop, telefoon, USB stick, waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, spoofing, besmetting met ransomware kunnen een datalek tot gevolg hebben.

Een datalek dient uiterlijk binnen 72 uur na ontdekking van het datalek te worden gemeld aan de toezichthouder. Indien dit later gebeurt, dan dient de melding voorzien te worden van uitleg omtrent de vertraging.

Niet ieder datalek-incident valt onder de meldplicht. Er is sprake van een zogeheten geclausuleerde meldplicht voor datalekken. Hiervoor is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Artikel 33(1) van de AVG stelt dat een datalek alleen gemeld dient te worden wanneer er een aanzienlijk risico is op schade aan de persoonlijke levenssfeer van een individu. Als bijvoorbeeld verloren of gesloten persoonsgegevens goed versleuteld zijn opgeslagen, dan is er geen aanzienlijke risico op schade aan de persoonlijke levenssfeer.

1.2 Doel en reikwijdte

Deze procedure beschrijft de wijze waarop binnen Constant IT wordt omgegaan met de meldplicht datalekken in de zin van de Algemene Verordening Gegevensbescherming (AVG).

Het bevat afwegingskaders bij een vermoeden van een datalek en specificeert de nodige acties.

Binnen Constant IT worden de volgende stappen in de procedure gehanteerd:

1. Het signaleren, analyseren en registreren van incidenten waarbij er sprake is van een inbreuk op een beveiligingsmaatregel en persoonsgegevens betrokken zijn;
2. Het inhoudelijk beoordelen en onderzoeken van het incident of er op grond van de AVG sprake is van een datalek dat gemeld moet worden;
3. Het melden van het datalek aan de betrokkenen en toezichthouder;
4. Het nemen van maatregelen om het lek te dichten;
5. Het documenteren van het datalek.

Hieronder volgt een nadere uitwerking van deze procedure.

2 Procedure Datalek

2.1 Melden Incident

De meldplicht datalekken geldt voor de elke organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken, of met een informatiebeveiligingsincident, of een vermoeden hiervan dient dit te melden.

Indien een melding binnen komt bij Constant IT, dient deze geregistreerd te worden en waar nodig, opgevolgd.

De medewerker wordt verzocht het incident met alle relevante informatie aan te maken voorzien van de naam en contactgegevens van de melder. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de AP.

Indien de medewerker twijfelt of er sprake is van een incident of wat hij moet doen, dient hij dit direct met zijn direct leidinggevende op te nemen.

2.1.1 Registratie

Het incident wordt geregistreerd in Autotask.

Er wordt geanalyseerd of er bij het incident persoonsgegevens betrokken zijn. Indien de melding telefonisch is gedaan, vraagt de medewerker die de melding afhandelt dit na bij de melder.

Indien bij het beveiligingsincident persoonsgegevens betrokken zijn, is de ontvanger van het incident er verantwoordelijk voor dat de melding wordt gemeld aan zijn direct leidinggevende of wanneer deze niet beschikbaar is een lid van het Management Team (MT). De leidinggevende informeert vervolgens altijd het MT.

Het MT informeert vervolgens de contactpersoon bij de Opdrachtgever.

2.2 Beoordelen of er sprake is van een datalek

2.2.1 Beoordeling

Zo snel mogelijk na de melding van een incident beoordeelt een lid van het MT in samenwerking met de contactpersoon van de Opdrachtgever of er sprake is van een datalek dat valt onder de meldplicht van de AVG. Indien wordt geconstateerd dat er sprake is van een meldenswaardige datalek, dan zorgt Constant IT in samenspraak met de Opdrachtgever voor opvolging van de melding door middel van een gemotiveerde beoordeling en een advies van het incident. Indien beoordeeld wordt dat het incident geen datalek in de zin van de AVG betreft, dan wordt dit teruggekoppeld aan de melder. De medewerker vult de oorspronkelijke melding in de registratie aan met de beoordeling van het incident.

De Opdrachtgever is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd naar de toezichthouder. Vanwege het gegeven dat een datalek binnen 72 uur gemeld dient te worden aan de toezichthouder dient de melding door alle betrokken medewerkers direct en met hoogste prioriteit te worden opgepakt. Ook wanneer een lek niet gemeld hoeft te worden, geldt een documentatieplicht. Binnen Constant IT wordt een register bijgehouden met daarin alle datalekken die zich voordoen.

2.2.2 Beslisboom voor de melding aan toezichthouder

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat alleen een inbreuk hoeft te worden gemeld als deze leidt tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van betrokkenen. Hierbij spelen de volgende factoren een rol:

1. Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals medische/ politiegegevens gegevens over ras of religie of financiële gegevens zijn gelekt.
2. Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

Er moet in ieder geval gemeld worden als één van onderstaande vragen positief wordt beantwoord.

- Zijn gegevens (definitief) verloren gegaan?
- Zijn de gegevens bijzonder of zeer omvangrijk?
- Zijn de gegevens in onbevoegde handen geraakt?
- Aanzienlijk risico op schade aan persoonlijke levenssfeer?

Is het antwoord op 1 (of meer) van bovenstaande vragen ja, dan dient het gemeld te worden. Is het antwoord op alle vragen nee, dan dient het niet gemeld te worden. Mogelijk is op het moment dat er gemeld moet worden nog geen volledig zicht op wat er gebeurd is

en om welke persoonsgegevens het gaat. In dat geval vindt de melding plaats op basis van de gegevens waarover men op dat moment beschikt. Eventueel kan de melding naderhand nog worden aangevuld of zelfs worden intrekken.

2.2.3 Melden aan betrokkene?

De betrokkene is degene over wie persoonsgegevens worden verwerkt en waarvan de gegevens onderwerp zijn van de datalek. Indien er sprake is van een datalek moet deze aan de betrokkene worden gemeld, als de inbreuk een hoog risico brengt op schade aan diens persoonlijke levenssfeer. Niet in alle gevallen hoeft een datalek aan de betrokkene te worden gemeld.

Voor de beoordeling of aan de betrokkene(n) gemeld moet worden, zijn de volgende vragen van belang. Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?

Zwaarwegende redenen:

- de nationale veiligheid, landsverdediging of openbare veiligheid
- de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, en de tenuitvoerlegging van straffen;
- andere belangrijke doelstellingen van algemeen belang van de Europese Unie of een lidstaat;
- de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
- een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
- de inning van civielrechtelijke vorderingen

Nee -> Melden betrokkene

Zijn de gegevens versleuteld of ontoegankelijk voor degene die geen recht op inzage heeft in deze gegevens?

Nee -> Melden betrokkene

Artikel 34(3) van de AVG stelt drie voorwaarden waaronder geen melding aan betrokkenen vereist is. Dit geldt in de volgende situaties:

1. Er zijn technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens vooraf aan het lek. In het bijzonder maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren.
2. Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen.

3. Het zou van onevenredige moeite zijn om contact op te nemen met individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel.

Termijn van melden voor het melden van een datalek aan betrokkenen geldt dat dit 'onverwijld' moet gebeuren. Uitgangspunt is dat onnodige vertraging wordt voorkomen, zodat de betrokkene de nodige maatregelen kan treffen. Gelet hierop dient een datalek binnen 72 uur te worden gemeld aan de toezichthouder. De wijze waarop betrokkenen worden geïnformeerd, bepaalt de Opdrachtgever zelf.

De Opdrachtgever is zelf verantwoordelijk voor het melden aan de betrokkene.

2.3 Melden aan andere partijen?

Indien er sprake is van samenwerking met andere partijen (ketenverwerking of verwerkers) zal er beoordeeld moeten worden of een datalek-incident aan de externe partij gemeld moet worden. Dit is geen wettelijke verplichting, maar kan vanuit communicatie redenen raadzaam zijn. Bij de uitwerking van de communicatiestrategie vindt afstemming plaats welke doelgroepen/overige partijen worden geïnformeerd over het datalek en op welke wijze. Ook in dit geval is de Opdrachtgever zelf verantwoordelijk voor het melden aan andere partijen.

2.4 Melden aan de toezichthouder en betrokkene(n)

De Opdrachtgever is ten alle tijde eindverantwoordelijk voor het voldoen aan de meldplicht datalekken. Op grond van de mandaatregeling meldt deze het datalek aan de toezichthouder en zorgt voor de verdere vervolgacties die kunnen voortkomen uit de melding.

Het is van belang dat bij een datalek de verantwoordelijken geïnformeerd worden. De noodzaak hiervan neemt toe, naarmate er sprake is van een incident waarbij veel partijen betrokken zijn en veel gevoelige informatie verloren is gegaan.

3 Afhandelen melding

Constant IT houdt een register bij van de meldingen van datalekken. In dit register verwerkt zij alle meldingen.

Deel II - 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): toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 AVG.

1.2 AVG: de Algemene verordening gegevensbescherming.

1.3 Data Processor: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.

1.4 Data Pro Statement: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, 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 Constant IT-diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt en zoals omschreven in het Data Pro Statement.

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 inaccessable), of, indien schriftelijk 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 daaropvolgende 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 soortgelijk 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

9.1 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