novaware

Verwerkersovereenkomst

Versie 1.0 – 24 mei 2018

DATA PRO CREATED BY NEDERLAND ICT

Novaware B.V.
Van Nagellstraat 2
8011 EB Zwolle
038-7114440
www.novaware.nl
info@novaware.nl

Standaard Verwerkersovereenkomst Novaware

Deze verwerkersovereenkomst van Novaware bestaat uit 2 delen:

- Deel 1. Data Pro Statement
- Deel 2. Standaardclausules voor verwerkingen

Deel 1: Data Pro Statement

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor de producten en diensten van Novaware.

1. Algemene informatie

1. **Dit Data Pro Statement is opgesteld door:**
   Novaware B.V.
   Van Nagellstraat 2
   8011 EB Zwolle

   KVK-nummer: 63590956
   BTW-nummer: NL855303682B01

2. **Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:**
   Martijn Maris
   info@novaware.nl
   038-7114440

3. **Dit Data Pro Statement geldt vanaf 24 mei 2018**
   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.

   De meest actuele versie kunt u op onze website www.novaware.nl vinden onder 'algemene voorwaarden'.

4. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van Novaware:**
    - Concept en creatie
    - Ontwikkeling en realisatie van online (maatwerk) oplossingen
    - Support en onderhoud (SLA) op door Novaware of door derden ontwikkelde oplossingen
    - Hosting

5. **Omschrijving van producten diensten**

    Novaware helpt bedrijven en organisaties die waarde willen creëren, met oog voor mensen en onze planeet. Het is onze ultieme uitdaging om juist voor deze bedrijven de online oplossing te realiseren die werkt en de juiste doelgroep raakt.

    Voor onze online oplossingen maken wij gebruik van het Umbraco content management systeem (CMS). Ook realiseren wij oplossingen op basis van .NET-technologie. Denk hierbij aan webapplicaties, websites, (klant)portalen, intranetten, koppelingen tussen systemen en apps.

    Elke door ons ontwikkelde oplossing kunnen wij voor opdrachtgever in onderhoud nemen waarbij wij opdrachtgever support kunnen leveren. De afspraken hiervoor leggen wij vast in een SLA. Voorbeelden van support zijn het beantwoorden van vragen van opdrachtgever en het maken van aanpassingen in de geleverde oplossingen.

    Opdrachtgever kan ervoor kiezen de gemaakte oplossing te hosten door Novaware. Wij gebruiken hiervoor het cloud-platform van Microsoft Azure.

6. **Beoogd gebruik**

    In de oplossingen die wij realiseren kunnen persoonsgegevens verwerkt worden van opdrachtgever en gebruikers. Voor de Umbraco-omgevingen die wij realiseren, geldt dat opdrachtgever zelf persoonsgegevens kan verzamelen door via de package Umbraco Forms formulieren aan te maken waar bezoekers of gebruikers van de omgeving hun gegevens in kunnen vullen.

    Voorbeelden van gegevens die door ons verwerkt kunnen worden in de (maatwerk) oplossingen voor opdrachtgever zijn:
    - NAW-gegevens waarbij meerdere adressen mogelijk zijn
    - Afbeeldingen en foto’s waarop één of meerdere personen kunnen staan
    - Titulatuur
    - Geslacht
    - Contactgegevens zoals: telefoonnummers en e-mailadressen
    - IP-adres
    - Links naar social media kanalen

- Inloggegevens waarbij de wachtwoorden zijn beveiligd
- Relaties met andere personen en organisaties
- Gekoppelde gegevens zoals: pagina's, nieuwsberichten en mediabestanden
- Gekoppelde documenten, persoonsgegevens of andere privacygevoelige informatie

Voor al onze diensten geldt dat tijdens onze werkzaamheden medewerkers in aanraking kunnen komen met gegevens die direct (zoals databestanden) of indirect (benaderbaar via applicaties) ter beschikking worden gesteld door derden of opdrachtgever. Al onze medewerkers zijn door werkgever geïnformeerd en zijn zich terdege bewust van de verantwoordelijkheid die zij dragen wanneer zij in aanraking komen met vertrouwelijke en/of privacygevoelige informatie en zullen hier te allen tijde zorgvuldig en discreet mee omgaan, zoals ook contractueel overeengekomen met werkgever.

Voor onze diensten geldt dat er geen rekening gehouden is met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

7. **Novaware heeft bij het ontwerpen van de producten en diensten privacy by design op de volgende wijze toegepast:**
   - Bij de realisatie van Umbraco-omgevingen werken wij volgens de security best practices van Umbraco. Meer informatie is te vinden op www.umbraco.com/security. Tevens adviseren wij opdrachtgever om de versie van Umbraco actueel te houden. Umbraco versie 7.9 en hoger voldoen aan de wettelijke kaders van de AVG / GDPR.
   - De pagina's en schermen die wij ontwikkelen in onze oplossingen bevatten standaard alleen die gegevens die nodig zijn voor de dienstverlening van de opdrachtgever. De opdrachtgever bepaalt welke velden beschikbaar zijn of niet. Novaware heeft hierin een adviseerde rol.
   - Opdrachtgever kan in onze oplossingen zelf bestanden uploaden in verschillende formaten (PDF, MS Word, MS Excel enz.) en kan gegevens in voorkomende gevallen zelf wijzigen en verwijderen.
   - Opdrachtgever kan, indien beschikbaar gesteld, zelf formulieren aanmaken in zijn Umbraco-omgeving waarmee persoonsgegevens worden verzamelt. Vanaf versie 7.9 van Umbraco CMS kan opdrachtgever ervoor kiezen de ingevulde formulieren, en daarmee ook eventuele persoonsgegevens, buiten het CMS op te slaan.
   - Novaware controleert de gegevens niet en zal gegevens alleen inzien op verzoek van de opdrachtgever, bijvoorbeeld als dat nodig is om support te kunnen leveren.

8. **Novaware gebruikt de Data Pro Standaardclausules voor verwerkingen. Deze zijn toegevoegd aan dit document en te downloaden vanaf onze website www.novaware.nl onder 'algemene voorwaarden'.**

9. **Novaware verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.**

10. **Novaware maakt gebruik van de volgende sub-processors:**
    - Microsoft Azure. Dit is de hostingprovider van Novaware waarbij hosting plaatsvindt binnen de EU. Microsoft Azure is ISO/IEC 27001:2013 gecertificeerd.
    - Umbraco Cloud. Zie ook: https://umbraco.com/products/umbraco-cloud/data-processing-agreement/

11. **Novaware ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
    Verzoeken voor inzage-, correctie- en het verwijderen van persoonsgegevens kunnen bij Novaware ingediend worden. De tijd en kosten die met deze verzoeken gepaard gaan, kunnen aan opdrachtgever in rekening worden gebracht.

    Verzoeken kunnen ingediend worden bij de supportdesk van Novaware. Dit geldt voor klanten met een actieve supportovereenkomst (SLA). In het geval van vragen betreffende AVG gerelateerde functionaliteiten in het systeem kan contact opgenomen worden met de supportdesk via support@novaware.nl 0f 038-7114440. Dit geldt ook voor vragen over:
    - Dataportabiliteit
    - Anonimisering
    - Pseudonimisering

12. **Na beëindiging van de overeenkomst met een opdrachtgever verwijdert Novaware de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**

2. Beveiligingsbeleid

13. Novaware heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:

- Novaware ontwikkelt met behulp van bewezen technologie.
- Novaware spant zich ervoor in dat elke oplossing veilig wordt opgeleverd. Dit houdt in dat maatregelen worden genomen om elke oplossing goed te beveiligen tegen de top-10 veiligheidsissues zoals deze door de Open Web Application Security Project (OWASP) wordt beschreven. Zie: https://www.owasp.org/index.php/Top_10_2013-Top_10.
- De hostingprovider van Novaware (Microsoft Azure) is ISO/IEC 27001:2013 gecertificeerd.
- De data die via de hostingprovider wordt opgeslagen staat fysiek in de EER (Europese Economische Ruimte).
- De infrastructuur zoals is ingericht binnen Microsoft Azure maakt gebruik van reverse proxies, (web application) firewalls, toegang op basis van IP-restricties en login / wachtwoorden. Alle communicatie met de eigen Novaware-servers is encrypted.
- De infrastructuur wordt up to date gehouden en actief gemonitored.
- Beveiligingsupdates aan (Umbraco) omgevingen worden altijd gemeld bij opdrachtgever en kunnen door Novaware doorgevoerd worden in de omgeving (bij een actieve SLA).
- Novaware adviseert opdrachtgever om de ontwikkelde oplossingen volgens security best practices te onsluiten. Denk hierbij aan SSL, het gebruik van sterke wachtwoorden en het afschermen van de Umbraco-backoffice op basis van 2-factor authenticatie en / of IP-restricties.
- Interne wachtwoorden zijn opgeslagen in een wachtwoordkluis met verschillende bevoegdheidsrollen en logging.
- Opdrachtgever kan kiezen voor dagelijkse back-up (tot 7 dagen terug) en uptime monitoring voor alle oplossingen die wij hosten.
- Optie om toegang te beperken via IP-restricties. Bijvoorbeeld de toegang tot de Umbraco-backoffice.
- Anonimiseren van persoonsgegevens in al onze test- en acceptatieomgevingen.
- Geheimhoudingsplicht voor alle medewerkers vastgelegd in een arbeidsovereenkomst.
- DKIM, SPF en DMARC zijn drie internetstandaarden die wij gebruiken om te voorkomen dat u uit onze naam e-mails ontvangt die virussen bevatten, spam zijn of bedoelt zijn om persoonlijke (inlog)gegevens te bemachtigen
- Medewerkerstoegang tot klantomgevingen en data op basis van need-to-know-principe
- Privacygevoelige gegevens slaan wij versleuteld op (met uitzondering van gegevens die via Umbraco Forms worden verzameld).

14. **Novaware heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**

    Novaware werkt zoveel mogelijk volgens de normen van ISO 27001 en is voornemens zich in de toekomst te conformeren aan ISO 27001 en NEN 7510.

15. **Novaware heeft de volgende certificeringen**
    - Novaware bechikt op het moment van schrijven nog niet over certificaten. Wij zullen onszelf certificeren met het het Data Pro Certificaat van Nederland ICT wanneer deze mogelijkheid geboden wordt.
    - De door Novaware ontwikkelde applicaties kunnen in opdracht van opdrachtnemer op veiligheid getest worden. Denk aan het uitvoeren van een penetration- of security test.
    - Novaware is Umbraco Gold Partner en volgt in de realisatie van Umbraco-omgevingen de best practices op security zoals vanuit Umbraco worden voorgeschreven.
    - Novaware is Microsoft Silver Partner en zorgt via opleidingen dat medewerkers van Novaware op de hoogte blijven van alle ontwikkelingen rondom security, privacy by default en het verwerken van persoonsgegevens.

3. Datalekprotocol

16. **In geval er toch iets mis gaat, hanteert Novaware het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**
    - Opdrachtgever heeft de verplichting tot het melden van Datalekken bij de AP, en in bepaalde gevallen, bij de Betrokkene op grond van artikel 33 en 34 van de AVG.
    - Om opdrachtgever te ondersteunen in het voldoen aan zijn verplichting tot het melden van datalekken, komen opdrachtgever en Novaware overeen dat Novaware opdrachtgever zo snel mogelijk zal informeren over beveiligingsincidenten, nadat Novaware voornoemde beveiligingsincidenten heeft ontdekt.
    - Novaware zal alle beveiligingsincidenten met betrekking tot de persoonsgegevens melden aan opdrachtgever. Dit gebeurt per e-mail. De melding wordt gericht aan het primaire contactpersoon van de opdrachtgever zoals deze bij Novaware bekend is. Opdrachtgever zal de ontvangst van de melding bevestigen. Novaware zal alle redelijke vragen van opdrachtgever met betrekking tot het beveiligingsincident beantwoorden.
    - De melding van een beveiligingsincident bevat zo mogelijk informatie over in elke geval de volgende onderwerpen:
        - Een samenvatting van het beveiligingsincident.
        - Informatie over de aard van het beveiligingsincident en welke categorieën persoonsgegevens en betrokkenen mogelijk door het incident worden geraakt.
        - Een antwoord op de vraag of persoonsgegevens verloren zijn gegaan dan wel bloot zijn gesteld aan onrechtmatige verwerking.
        - Informatie over de beveiligingsmaatregel waarop het beveiligingsincident betrekking heeft.
        - Informatie over de manier waarop het beveiligingsincident zich heeft voorgedaan.
        - Informatie over de oorzaak van het beveiligingsincident.
        - Informatie over te nemen en genomen vervolgacties door Novaware en reparatie van het beveiligingsincident.
    - Melding van datalekken aan de AP en betrokkenen, blijft te allen tijde de verantwoordelijkheid van opdrachtgever. Novaware is nimmer verplicht tot het melden van datalekken aan de AP en/of de betrokkene.
    - Novaware zal, waar mogelijk en nodig, zijn medewerking verlenen aan noodzakelijke informatievoorziening aan opdrachtgever in het kader van de door Novaware gemelde beveiligingsincidenten aan opdrachtgever. Novaware kan de extra kosten die zij in dit kader maakt in rekening brengen bij opdrachtgever.

4. Overeenkomst

Bij akkoord, ontvangt u per e-mail een uitnodiging om dit document digitaal te ondertekenen. Dit verloopt via onze partner Adobe Sign. Na ondertekening ontvangt u een kopie van het ondertekende document per e-mail.

Opdrachtgever:	(Sub) Verwerker:
Datum en plaats:	Datum en plaats:
Handtekening:	Handtekening:

DEEL 2: STANDAARDCLAUSULES VOOR VERWERKINGEN

versie: januari 2018

Vormt samen met het Data Pro Statement de verwerkersovereenkomst en is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden

ARTIKEL 1. DEFINITIES

Onderstaande begrippen hebben in deze Standaardclausules voor verwerkingen, in het Data Pro Statement en in de Overeenkomst de volgende betekenis:

1.1 **Autoriteit Persoonsgegevens (AP):** 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 de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.

1.8 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.

1.9 **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 Avg.

ARTIKEL 2. ALGEMEEN

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.

2.2 Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.

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

2.4 Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de Avg, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de Avg en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de Avg zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de Avg voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de Avg handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Data Processor.

ARTIKEL 3. BEVEILIGING

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico's en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

ARTIKEL 4. INBREUKEN IN VERBAND MET PERSOONSGEGEVENS

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 Avg) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

4.2 Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 Avg moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 Avg.

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

ARTIKEL 5. GEHEIMHOUDING

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

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

ARTIKEL 6. LOOPTIJD EN BEËINDIGING

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

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

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de Avg is ten aanzien van de Persoonsgegevens.

ARTIKEL 7. RECHTEN DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENT (DPIA) EN AUDITRECHTEN

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 Avg.

7.3 Data Processor kan de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige.

7.4 Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de Avg of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.5 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.6 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

ARTIKEL 8. SUBVERWERKERS

8.1 Data Processor heeft in het Data Pro Statement vermeldt of, en zo ja welke derde partijen (subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere subverwerkers in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

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

wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

ARTIKEL 9. OVERIG

Deze Standaardclausules voor verwerkingen vormen tezamen met het Data Pro Statement een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst.