Data Pro Statement en Verwerkersovereenkomst

Versie 1.6 - 03 / 2024

Monitor Volwassenen Educatie

QWASP B.V.

Deel 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor het product of de dienst van Qwasp BV, verder te noemen Qwasp of Data Processor.

ALGEMENE INFORMATIE

1. Dit *Data Pro Statement* is opgesteld door Qwasp, Monseigneur Borretstraat 63, 5375 AB Reek. Voor vragen over dit Data Pro Statement kan contact opgenomen worden met Jan van de Wetering, **T** *(06) 4229 2997*, **E** *j.wetering@qwasp.eu*

   Voor technische vragen over dataprotectie kan contact worden opgenomen met Roeland Verhulsdonck, **T** *(06) 1434 1424*, **E** *r.verhulsdonck@qwasp.eu*

2. Dit Data Pro Statement geldt vanaf 1 juli 2020. De in dit Data Pro Statement omschreven beveiligingsmaatregelen passen wij zo nodig 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 Data Pro Statement is ook te raadplegen op **www.monitorvolwasseneneducatie.com** onder de knop 'beveiliging'.

Qwasp BV

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van Qwasp: de registratiemodule en vaardighedentoetsen (leestoetsen, schrijftoetsen, rekentoetsen en digitale vaardighedentoetsen) van de Monitor Volwasseneneducatie.

4. Omschrijving product/dienst
   Qwasp helpt organisaties om persoonsgegevens van cursisten vast te leggen en het leerniveau te monitoren.

5. Beoogd gebruik van de modules: om de in de Web opgenomen verplichting te zorgen voor een aanbod opleidingen educatie met voldoende aandacht voor alle doelgroepen uit te voeren en de deelnemers aan leertrajecten te kunnen begeleiden en ondersteunen, willen de gemeenten persoonsgegevens verzamelen die daarvoor noodzakelijk zijn. Met de registratiemodule hebben gemeenten de mogelijkheid om van deelnemers te registreren wie ze zijn, welke cursus een deelnemer volgt of heeft gevolgd en met welk resultaat en hoe een deelnemer te bereiken is. De kwantitatieve gegevens worden gebruikt om verantwoording over de uitvoering van de taak opgenomen in de Web af te leggen aan de Minister. De resultaten van vaardighedentoetsen kunnen door de gemeente ook gebruikt worden om de kwaliteit van het volwassenenonderwijs is beeld te krijgen, zodat de doelmatigheid van de taak bevorderd wordt. Het resultaat van een toets kan ook worden gebruikt om de deelnemer naar de meest geschikte educatie te leiden. Met de toetsen leesvaardigheid, schrijfvaardigheid, rekenvaardigheid en digitale vaardigheden wordt een of worden meerdere vaardigheden gemeten. Nadat de deelnemer de educatie heeft gevolgd, kan de bereikte leeruitkomst worden gemeten.

Het gaat dan om adresgegevens, geslacht, leeftijd en ook:

- Wel of niet in Nederland geboren (NT1/NT2)
- Begin- en einddatum educatietraject
- Type traject
- Type docent
- Educatievorm (formeel/non-formeel)
- Begin- en eindniveau deelnemer, voor en na gevolgde educatietraject

Taalinstellingen, ROC's en taalhuizen kunnen de modules gebruiken om de vaardigheid van deelnemers aan educatie vast te stellen en de voortgang te monitoren.

Bij deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. Verwerken van deze gegevens met het hiervoor beschreven product of dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. Qwasp heeft bij het ontwerpen van de monitor volwasseneneducatie *privacy by design/privacy by default* op de volgende wijze toegepast:
   - De schermen bevatten alleen die gegevens die nodig zijn voor de begeleiding en ondersteuning van de deelnemer;
   - De gegevens worden waar mogelijk gepseudonimiseerd (zo wordt de naam van een betrokkene vervangen door een persoonlijke code);
   - Open invulvelden zijn niet toegestaan;
   - De bevoegdheden van gebruikers zijn zoveel mogelijk beperkt, zodat alleen gebruikers die bepaalde persoonsgegevens nodig hebben voor de uitvoering van hun werkzaamheden toegang hebben;
   - Betrokkenen vullen gegevens in nadat ze geïnformeerd zijn waar de gevraagde gegevens voor worden gebruikt, en nadat ze zijn geïnformeerd over de grondslag die de verwerkingsverantwoordelijke heeft aangewezen voor de gegevensverwerking. Een betrokkene kan zijn op grond van toestemming verwerkte gegevens wijzigen of verwijderen, zonder tussenkomst van de verwerker;
   - Qwasp heeft een verwijderfunctie ingebouwd, zodat gegevens eenvoudig kunnen worden verwijderd op instructie van de verwerkingsverantwoordelijke.

7. Qwasp gebruikt de standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn (Deel 2).

8. De module verwerkt alleen persoonsgegevens in de Europese Unie.

9. Qwasp maakt gebruik van de volgende sub-processors:
   - *Microsoft Azure*:
     Qwasp levert haar software middels het model SaaS, Software as a Service. Qwasp gebruikt in deze SaaS oplossing een Learning Management System gekoppeld aan een My SQL Database. De servers van Qwasp worden gehost in private cloud binnen de Microsoft Azure cloud. Hiervoor worden ISO 27001gecertificeerde datacenters binnen de EU gebruikt. Qwasp kiest voor Microsoft Azure omdat onze SaaS oplossing op deze datacenters het hoogste veiligheidsniveau biedt. Biometrische toegangsbeveiliging, 24/7 fysieke beveiliging, videosurveillance, alarmsystemen, brandbeveiliging alsmede extra energievoorzieningen om stroomuitval op te vangen.
   - *Copaco*:
     hiernaast heeft Qwasp voor haar ondersteuning bij de integratie en opslag van data bij de door Microsoft Azure geleverde clouddiensten Copaco NV, gevestigd in

Eindhoven, ingeschakeld. Copaco ondersteunt Qwasp in de mogelijkheden bij Microsoft Azure en helpt bij de opbouw van de ICT infrastructuur. Copaco zelf heeft ook geen toegang tot de data. De support-afdeling kan wel inloggen in de online-omgeving, maar kan daar alleen de gegevens van Qwasp zelf inzien en ondersteunen bij onder andere de instellingen van haar dienst. De data zelf kan niet worden ingezien. Alleen enkele medewerkers van Copaco, zoals een CTO of een hoofd-support medewerker, hebben een algemeen admin-account, waarmee zij meer support kunnen leveren indien dat noodzakelijk is om de juiste beveiliging van haar dienst te kunnen blijven garanderen en alleen in het geval dat daarvoor een opdracht van Qwasp is ontvangen.

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
    de betrokkene heeft het recht op informatie over de verwerking van zijn gegevens, over welke gegevens het gaat, hoe ze worden verwerkt, waarom en door wie. De betrokkene heeft het recht om gegevens die over hem worden verwerkt in te zien, heeft het recht op een kopie van de over hem verwerkte persoonsgegevens, heeft het recht om gegevens die incorrect zijn aan te (laten) passen en gegevens die onvolledig zijn, aan te (laten) vullen). Wanneer gegevens onrechtmatig worden verwerkt, mag de betrokkene vragen daarmee te stoppen of te vragen de gegevensverwerking te beperken.
    De data verwerkende organisatie zal in principe altijd aan een verzoek van een betrokkene gehoor geven.
    De verwerkingsverantwoordelijke kan zelf een kopie maken van de gegevens die over een betrokkene worden verwerkt en deze kopie aan de betrokkene verstrekken.
    Wanneer data incorrect of onvolledig zijn, mag een betrokkene vragen ze aan te passen.
    Een betrokkene kan altijd, indien toestemming als grondslag voor het verwerkingsproces is aangewezen, zijn toestemming intrekken. In dat geval worden de gegevens gewist.

    De opdrachtgever als verwerkingsverantwoordelijke kan Qwasp instructie geven bij de afhandeling van een verzoek te assisteren. Qwasp zal zo'n verzoek steeds binnen vijf werkdagen afhandelen en de opdrachtgever informeren. De contactpersoon kan via de helpdesk een ticket aanmaken met verzoeken om een export, aanpassing of verwijdering van gegevens. De kosten hiervoor bedragen € 5,00 exclusief BTW per verzoek.

11. Na beëindiging van de overeenkomst met een opdrachtgever verwijdert Qwasp 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).

12. De opdrachtgever kan verzoeken om de persoonsgegevens van een of meerdere betrokkenen tijdens de duur van de overeenkomst en ook na het einde van de overeenkomst (niet na het einde van de door de verwerkingsverantwoordelijke vastgestelde bewaartermijn) over te dragen aan een andere leverancier van hetzelfde soort dienst of aan de verwerkingsverantwoordelijke zelf. De gegevens worden dan in een machineleesbare vorm verstrekt zonder kosten.

Beveiligingsbeleid

13. De persoonsgegevens worden gepseudonimiseerd door bij de intake (de eerste registratie) elke deelnemer een Intake-Deelnemer nummer ('I-D') te verstrekken. Dit ID-nummer is tevens de loginnaam.

    Om te voldoen aan de 3 2 1 regels voor back-up worden onze off-site back-ups ook opgeslagen binnen Nederland op servers buiten de Microsoft Azure Cloud op twee locaties.

    Qwasp heeft gekozen voor een multi-tenant ontwerp zodat er toegang voor delen van het bedrijfsproces kan worden ontzegd of het hele proces kan worden gestopt zonder dat door andere tenant onderdelen stagneren. Bij een langdurige storing van de Azure Cloud is er een uitwijkomgeving beschikbaar op twee Virtual Private Servers in het hostnet netwerk. De verdeling van de omgevingen is weergegeven in een schema. Dit schema wordt bijgewerkt bij wijzigingen en is beschikbaar op verzoek in het dossier processen en afspraken.

    Communicatie tussen gebruikers van de monitor en onze software wordt geëncrypt via HTTPS en Transport Layer Security (TLS). Het certificaat nodig voor het beveiligen van het domein qwasp-apps.com is ondergebracht in een Microsoft Keyfault. Een Azure kluis voor certificaten en geheimen.

    Het Disaster Recovery (DR)-programma verzekert dat onze dienstverlening en softwareproducten ook bij grote incidenten beschikbaar blijven of zo snel mogelijk weer beschikbaar kunnen worden gemaakt.

    Alle medewerkers van Qwasp die toegang hebben tot persoonsgegevens hebben in hun arbeidsovereenkomst een geheimhoudingsverklaring en integriteitsverklaring getekend en zullen gedurende hun dienstverband en daarna op verantwoorde wijze met informatie omgaan.

14. Qwasp heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):
    - De Baseline Informatiebeveiliging Overheid (BIO) v1.04
    - NEN-ISO 27001
    - OWASP
15. Data processor heeft de volgende certificeringen:
    - Data Pro Certificate

Protocol informatiebeveiligingsincidenten en datalekken

16. Qwasp heeft een protocol beveiligingsincidenten (het datalekken protocol) opgesteld, waarin de procedures zijn beschreven die moeten worden gevolgd in het geval een datalek (inbreuk in verband met persoonsgegevens) wordt geconstateerd. Het protocol is te raadplegen op de site onder de knop beveiliging.

Qwasp zal opdrachtgever zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) inbreuk. Qwasp zal zelf geen meldingen doen aan de Autoriteit Persoonsgegevens of aan betrokkene(n). Wel of niet melden blijft de verantwoordelijkheid van opdrachtgever. Qwasp zal opdrachtgever desgewenst ondersteunen bij het meldproces.

Deel 2: Standaardclausules voor verwerkingen
Versie: september 2019

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, sub-processors, 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.

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 of door de overheid uitgegeven persoonsnummers.

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 aan 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 zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

7.4 Data Processor 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 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.

7.6 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. 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.

7.7 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. Sub-Processors

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

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere sub-processors 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.