Versie: oktober 2026

Verwerkers-overeenkomst Teqa Informatica B.V.

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

NLdigital versie maart 2025

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 het bedrijf dat dit Data Pro Statement heeft opgesteld.

Algemene informatie

1. **Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):**
   Teqa Informatica B.V.
   Reykjavikstraat 1
   3543 KH
   Utrecht
   Nederland
   Hierna te noemen ‘data processor’.

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   J.W. Snijders
   Postbus 4
   3540 AA
   Vleuten
   privacy@teqa.eu
   +31 030 237 3030

2. **Dit Data Pro Statement geldt vanaf** *01-oktober-2026*
   Dit Data Pro Statement en de daarin 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 producten en diensten van data processor**
   i-Reserve

4. **Omschrijving product(en)/dienst(en)**
   Teqa opereert in de informatietechnologiesector en is de leverancier van een aanpasbare applicatie voor reserveringsbeheer, i-Reserve genaamd. Teqa levert i-Reserve volgens een Software as a Service (SaaS) model. De i-Reserve-dienst vergemakkelijkt de boeking / organisatie van objecten of activiteiten in een breed scala van sectoren. Momenteel zijn de belangrijkste klanten van Teqa bedrijven die boekbare opties aanbieden op het gebied van sport en fitness, rondleidingen, trainingen, cursussen, vergaderruimtes en entertainmentactiviteiten. Teqa ontwikkelt, levert en implementeert i-Reserve zelf. De infrastructuur waarop i-Reserve draait, wordt beheerd door Teqa of door een door Teqa geselecteerde hostingpartij (zie bepaling 9). Teqa adviseert en ondersteunt haar klanten ook bij het gebruik van de geleverde software.

5. **Beoogd gebruik**

Product/dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:
i-Reserve software biedt een verscheidenheid aan standaard en aangepaste velden die kunnen worden gebruikt om informatie te verzamelen, zoals NAW gegevens, e-mailadressen, telefoonnummers, interesses, opleidingsniveau, voorkeuren, afspraken, facturatiegegevens, inhoud e-mailverkeer en andere communicatie met de klant. Teqa heeft niet de controle over welke informatie u wilt verzamelen.

Sla geen bijzondere persoonsgegevens op. Teqa raadt je ten zeerste af om bijzondere persoonsgegevens in onze software vast te leggen. Denk aan: gegevens over gezondheid, gegevens waaruit de etnische en/of religieuze afkomst afleidbaar is, BSN-nummers, genetische gegevens etc. Technisch kunnen wij niet afdwingen dat je geen bijzondere persoonsgegevens opslaat of verstuurt, aangezien je daar zelf de controle over hebt. Maar we raden het opslaan van dit type persoonsgegevens ten strengste af.

Bij dit product/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. Indien u toch bijzondere persoonsgegevens verwerkt, dan kunt u het beste uw privacy officer contact met ons op laten nemen om eventuele aanvullende mogelijkheden te bespreken. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is altijd ter eigen beoordeling door opdrachtgever.

6. **Privacy by design/privacy by default**

Bij de ontwikkeling en het onderhoud van i-Reserve past data processor de beginselen van privacy by design en privacy by default toe.

Dit betekent onder meer dat:

- standaard alleen de velden verplicht zijn die nodig zijn om een reservering te maken;
- aanvullende velden, waaronder vrij in te richten velden, optioneel zijn en door opdrachtgever zelf worden ingericht en ingeschakeld;
- toegangsrechten binnen i-Reserve rolgebaseerd kunnen worden ingericht, zodat uitsluitend geautoriseerde gebruikers toegang hebben tot persoonsgegevens;
- gegevensoverdracht plaatsvindt via beveiligde verbindingen (HTTPS/SSL);
- functionaliteiten beschikbaar zijn voor het verwijderen van persoonsgegevens en voor het automatisch anonimiseren daarvan. Opdrachtgever stelt zelf in welke gegevens worden geanonimiseerd. Of gegevens daarna niet meer tot een persoon te herleiden zijn, hangt af van die instelling: blijven bijvoorbeeld geboortedatum en postcode bewaard, dan kan een persoon mogelijk nog worden herleid;
- logging- en monitoringmechanismen worden toegepast ter detectie van ongeautoriseerde toegang;
- nieuwe functionaliteiten vooraf worden beoordeeld op privacy- en beveiligingsrisico's.

Opdrachtgever is onder andere verantwoordelijk voor:

- het beperken van de invoer van persoonsgegevens tot hetgeen noodzakelijk is;
- het correct configureren van autorisaties en bewaartermijnen;
- het inrichten van aanvullende velden en van de instellingen voor automatisch anonimiseren.

Data processor faciliteert privacyvriendelijke instellingen, maar heeft geen zeggenschap over de concrete inrichting en het gebruik van het systeem door Opdrachtgever.

7. **Data processor gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn.**

8. **Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER**.

9. **Data processor maakt gebruik van de volgende sub-processors:**
De meest actuele stand is terug te vinden op https://teqa.nl/data-pro-statement
   - Leaseweb Netherlands B.V. – hosting van databases, webservers en bestandsopslag
     Locatie verwerking: Nederland (EU)
     Certificeringen: ISO 9001, ISO 27001
   - Mailgun (Sinch) – verzending van e-mail vanuit i-Reserve (o.a. bevestigingen en notificaties), via de EU-regio van Mailgun
     Locatie verwerking: EU
   - Acronis – opslag van back-ups
     Locatie verwerking: datacenter Frankfurt, Duitsland (EU)

   i-Reserve kan worden gekoppeld met producten van externe partijen, zoals Exact, King, Accountview, Cardgate, Mollie, Buckaroo, Google kalenders en anderen. Indien i-Reserve wordt gekoppeld met producten van dergelijke externe partijen, is Opdrachtgever zelf verantwoordelijk voor het maken van afspraken met deze externe partijen omtrent de verwerkingen van persoonsgegevens.

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
In i-Reserve is het mogelijk dat uw klant zelf zijn/haar gegevens kan inzien, corrigeren, verwijderen of downloaden. De beheerder kan ook zelf klantgegevens exporteren of via een API gegevens doorsturen.
In het geval dat een betrokkene een verzoek tot uitoefening van zijn/haar wettelijke rechten richt aan data processor, zal data processor het verzoek doorsturen aan opdrachtgever, en dient opdrachtgever het verzoek verder af te handelen. Data processor mag de betrokkene daarvan op de hoogte stellen.

11. **Data processor ondersteunt opdrachtgever op de volgende manier bij Data Protection Impact Assessments (DPIA's):**
Indien opdrachtgever daartoe verplicht is, zal data processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een Data Protection Impact Assessment (DPIA) of een daarop volgende voorafgaande raadpleging, zoals bedoeld in artikel 35 en 36 AVG.
Een verzoek hiertoe kan worden gericht aan privacy@teqa.eu. Data processor stelt daarbij de informatie ter beschikking die in redelijkheid van hem verwacht mag worden, zoals een beschrijving van de verwerkingen binnen i-Reserve, de getroffen technische en organisatorische beveiligingsmaatregelen (bepaling 14), de ingeschakelde sub-processors (bepaling 9) en de locatie van de verwerking (bepaling 8).
Data processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij opdrachtgever, conform artikel 7.7 van de Standaardclausules voor verwerkingen.

12. **Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt binnen *3 maanden* op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**
Dit geldt ook voor back-ups: back-ups worden eveneens binnen 3 maanden na beëindiging van de Overeenkomst verwijderd.

13. **Retourneren van persoonsgegevens na beëindiging van de Overeenkomst**
Na beëindiging van de overeenkomst met opdrachtgever kan data processor op verzoek alle persoonsgegevens die hij voor opdrachtgever verwerkt binnen 3 maanden aanleveren op een door opdrachtgever aangeleverde datadrager.

Beveiligingsbeleid

14. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
Alle gegevens worden verwerkt binnen de EU/EER
- Programmacode in eigen beheer
- Mogelijkheid tot twee-staps-verificatie voor toegang tot i-Reserve
- Minimumeisen aan samenstelling wachtwoorden
- Veilige HTTPS verbinding met SSL certificaat
- Versleuteling van informatie
- Web Application Firewall (WAF)
- IP adres whitelisting voor beheerfuncties
- Slowdown en lockdown mechaniek
- Scans en backups
- Mogelijkheid om persoonsgegevens automatisch te anonimiseren, door opdrachtgever in te stellen (zie bepaling 6)
- Hostingpartners voldoen aan ISO 9001, ISO 27001
- Medewerkers van data processor zijn gehouden aan een geheimhoudingsplicht
- Medewerkers van data processor worden getraind op informatiebeveiligingsbewustzijn

Een samenvatting en meest actuele stand van de beveiligingsmaatregelen vindt u op:
https://support.i-reserve.net/nl/algemene-informatie/wat-doet-i-reserve-aan-beveiliging-en-privacy-van-persoons-gegevens/

15. **Data processor heeft zich geconformeerd aan een Information Security Management System (ISMS):**

- ISO 27001
- ISMS NLdigital

16. **Data processor heeft de volgende verificaties en certificeringen:**

- Data Pro Verified

Datalekkenprotocol

17. **In geval er toch iets mis gaat, hanteert data processor het volgende datalekkenprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**
    - In het geval van een inbreuk in verband met persoonsgegevens zal data processor u daarover zonder onredelijke vertraging informeren. Data processor spant zich naar beste kunnen in om ervoor te zorgen dat de verstrekte informatie volledig, correct en accuraat is.
    - Opdrachtgever beoordeelt zelf of hij de toezichthoudende autoriteiten en/of betrokkenen zal informeren of niet.
    - De melding van data processor behelst in ieder geval het melden van het feit dat er een lek is geweest, alsmede, voor zover de informatie voorhanden is:
        - wat de (vermeende) oorzaak is van het lek;
        - contactgegevens voor de opvolging van de melding;
        - bij benadering: het aantal betrokkenen en registers van persoonsgegevens;
        - wat is het (vooralsnog bekende en/of te verwachten) gevolg;
        - wat is de (voorgestelde) oplossing;
        - wat de reeds ondernomen maatregelen zijn.

Data processor gebruikt de volgende monitoring tools/werkwijze om potentiële beveiligingsincidenten te signaleren: De monitoring wordt gedaan door Leaseweb, het hostingbedrijf van onze servers. Leaseweb is ISO27001 gecertificeerd, hierin wordt de informatiebeveiliging / monitoring onderbouwd.

Deel 2: Standaardclausules voor verwerkingen

Versie: maart 2025

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.