



VERWERKERS- OVEREENKOMST ***DATAPROFIT B.V.***

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Versie *1.0 / 22-05-2018*>

DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkerovereenkomst voor het product of de dienst van DataProfit B.V. BV dat dit Data Pro Statement heeft opgesteld.

ALGEMENE INFORMATIE

1. Dit Data Pro Statement is opgesteld door DataProfit B.V. BV (hierna te noemen DataProfit B.V.), gevestigd op Bos en Lommerplantsoen 1, 1055 AA te Amsterdam. Voor vragen over dit Data Pro statement of dataprotectie kan contact opgenomen worden met Sander van der Burg, sander.vandenburg@dataprotitssc.nl.
2. Dit Data Pro Statement geldt vanaf 20 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.
3. Dit Data Pro Statement is van toepassing op het product DataProfit Insights. DataProfit Insights wordt ontwikkeld en geproduceerd door DataProfit BV (hierna te noemen DataProfit).
4. DataProfit Insights is een web-based Business Intelligence (BI) platform waarmee gestuurd kan worden op basis van operationele en management indicatoren, hetgeen gerealiseerd wordt door het aansluiten van verschillende databronnen op het DataProfit platform. De producten kunnen via een breed scala aan webbrowsers gebruikt worden doormiddel van het invoeren van een unieke URL.
5. DataProfit Insights is zo ontworpen dat het op twee manieren persoonsgegevens kan verwerken, te weten gebruikersgegevens en persoonsgegevens van werknemers van zakelijke klanten. Zie voor een gedetailleerde lijst [Bijlage 1](#).
6. Bij dit product is 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 door opdrachtgever is ter eigen beoordeling door opdrachtgever.
7. DataProfit B.V. gebruikt de Data Pro Standaardclausules voor eigen verwerkerovereenkomst welke op te vragen is via info@dataprotitssc.nl.
8. DataProfit B.V. verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.

9. Data processor maakt gebruik van de volgende sub-processors:
- ✚ DataProfi: DataProfit B.V. vraagt bij DataProfit, op basis van de klantgegevens, een klant specifieke omgeving aan waarop ingelogd kan worden door de klant. Deze gegevensoverdracht gaat via een versleutelde (https) verbinding (STACK). DataProfit gebruikt op haar beurt de Europese Amazon servers om de klant omgevingen te hosten. Deze subverwerker is gesitueerd binnen de EU/EER, te weten Nederland. Zie verder www.dataprofit.com.
 - ✚ STACK: STACK is een encrypted cloud omgeving welke gebruikt wordt door DataProfit B.V. om onder andere contracten, klantgegevens en gebruikersgegevens op te slaan. Dit ten behoeve van de klant-leverancier relatie, support en administratie. De gegevens worden versleuteld met het AES 256-bit protocol en de verbinding loopt altijd via HTTPS;. Zie verder <https://www.transip.nl/legal-and-security/privacy-policy/> en <https://www.transip.nl/knowledgebase/artikel/268-de-privacy-en-encryptie-stack/>.
10. Na beëindiging van de overeenkomst met een opdrachtgever verwijdert DataProfit B.V. de persoonsgegevens die hij voor de opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn ('render inaccessible').

BEVEILIGINGSBELEID

11. Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:
- ✚ Persoonsgegevens worden niet geanonimiseerd.
 - ✚ DataProfit Insights is een web-based oplossing. De gebruiker dient zich aan te melden via een login portal welke bij het bezoeken van de specifieke klant omgeving zichtbaar wordt. Authenticatie tussen de server en de client, bij het inloggen op de klant specifieke omgeving, gebeurt middels het SSL protocol. Binnen de omgeving van de klant kunnen gebruikers aangemaakt worden met specifieke rechten op de omgeving zoals het inzien van omzet gegevens. Alle omgevingen worden gehost op de Amazon servers waar alleen de administrators van DataProfit op in kunnen loggen. Door IP-filtering voor toegangsrecht toe te passen is een extra beveiliging ingebouwd wat betekent dat alleen bevoegden, vanuit het private DataProfit netwerk, op de administrator omgeving van de Amazon server in kunnen loggen. De administrator inloggegevens zijn alleen bekend bij de ontwikkelaars van DataProfit.
 - ✚ DataProfit B.V. levert per klant omgeving een algemene (hoofd) gebruiker op aan een klant. Op verzoek kunnen meerdere gebruikers binnen een omgeving aangemaakt worden. Wanneer de klant dit wenst kunnen de rechten van een specifieke gebruiker ingetrokken worden of kan zelfs de toegang volledig ontzegt worden.
 - ✚ Klanten van DataProfit B.V. zijn zelf verantwoordelijk voor het bewaren van logingegevens. Wanneer deze verloren zijn gegaan kan de klant zelf een herstel procedure starten via zijn of haar eigen omgeving.

- ✚ De databases op de Amazon server doorloopt dagelijks een back-up procedure om te zorgen, dat wanneer een calamiteit zich voordoet, de toegang tot de data tijdig hersteld kan worden.

DataProfit B.V. maakt verbinding via het internet met de Amazon server. Deze verbindingen zijn altijd versleuteld met behulp van het SSL protocol, hetgeen betekent dat het onderscheppen van de gegevens welke over de verbinding gaan, nagenoeg onmogelijk is. Daarnaast gebruikt DataProfit B.V. een encrypted cloud omgeving, welke is versleuteld met de AES-256 bits standaard, voor de opslag van data. Deze opslag wordt elke 4 uur geback-upt.

DATALEKPROTOCOL

12. In geval er toch iets mis gaat, hanteert DataProfit B.V. het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten.

DataProfit B.V. hoeft in haar rol als verwerker niet te bepalen of een inbreuk gemeld moet worden aan de AP en/of betrokkenen en hoeft ook de melding niet te doen. DataProfit B.V. zal wel:

- ✚ bij detectie van inbreuk waar persoonsgegevens bij betrokken zijn wordt dit zonder onredelijke vertraging gemeld aan de verantwoordelijke;
- ✚ de verantwoordelijke te ondersteunen/assisteren zover zij dit kan bij het voldoen aan de op de verantwoordelijke rustende verplichtingen.

Er is sprake van een ‘inbreuk in verband met persoonsgegevens’ (hierna: datalek) als er een inbreuk is op de beveiliging die als gevolg heeft:

- ✚ vernietiging van persoonsgegevens (bijvoorbeeld door brand of wissen); of
- ✚ verlies van persoonsgegevens (bijvoorbeeld USB of laptop die kwijtraakt); of
- ✚ wijziging van persoonsgegevens (zonder dat dit de bedoeling was); of
- ✚ ongeoorloofde verstrekking van persoonsgegevens (bijvoorbeeld e-mail/bestanden verzonden aan verkeerde geadresseerde); of
- ✚ ongeoorloofde toegang tot doorgezonden/opgeslagen/anderszins verwerkte persoonsgegevens (bijvoorbeeld door een hacker of een niet-bevoegd personeelslid).

Bij de hierboven beschreven situaties maakt het niet uit of er sprake is van opzet (zoals een hacker die zich ongeoorloofd toegang verschaft tot persoonsgegevens) of dat per ongeluk iets mis gaat (het per ongeluk wissen van gegevens die in tact moesten blijven). Wanneer er geen gevolgen zijn voor de persoonsgegevens spreken wij niet van een datalek.

DataProfit B.V. bewaakt alleen haar eigen clients op datalekken, zij bewaakt niet klant specifieke omgevingen. Indien DataProfit B.V. intern een datalek constateert, doorloopt DataProfit B.V. het volgende protocol:

1. Wanneer DataProfit B.V. een datalek constateert of wanneer een sterk vermoede heerst, zal het crisisteam worden opgeroepen. Het crisis team van DataProfit B.V. bestaat uit een vertegenwoordiger van het management en een externe IT-specialist. De eerste prioriteit van dit team is maatregelen nemen om dit datalek te stoppen en de gevolgen te beperken. Daarnaast draagt dit team zorg voor het doorspelen van de juiste informatie aan de betrokken partijen.
2. Indien geconstateerd wordt dat het lek nog niet gedicht is worden maatregelen getroffen om het lek alsnog te stoppen. Wanneer DataProfit B.V. zelf het lek niet weet te dichten wordt de hulp ingeschakeld van een specialist. Vervolgens worden maatregelen getroffen om de data veilig te stellen en bewijsmateriaal te verzamelen.
3. Vervolgens wordt het datalek onderzocht en gedocumenteerd op de volgende onderwerpen: type incident, beschrijving incident, eventuele (sub)verwerker, om hoeveel personen het gaat, omschrijving van de groep personen, wanneer het incident plaatsvond, aard van het incident, type persoonsgegevens, welke gevolgen dit heeft voor de betrokkenen, vervolgacties om herhaling te voorkomen, technische maatregelen die zijn getroffen en geografische impact. Daarnaast zal in deze fase worden geïnventariseerd welke klanten van DataProfit B.V. hierdoor zijn getroffen.
4. De klanten die zijn getroffen zullen door DataProfit B.V. zonder onredelijke vertraging via e-mail worden geïnformeerd over het datalek door contact op te nemen met de bij DataProfit B.V. geregistreerde hiervoor te benaderen contactpersoon (of indien dit niet specifiek bekend is, de algemeen geregistreerde contactpersoon). Op basis van deze informatie kan de klant beoordelen of het datalek gemeld moet worden bij de AP.
5. In de laatste fase van het protocol zal het crisisteam inventariseren hoe een soortgelijk datalek kan worden voorkomen in de toekomst.

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):** toezichhoudende 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 inaccessible*), 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.

BIJLAGE 1: LIJST PERSOONSgegevens

Gebruikersgegevens:

- *Gebruikersnaam*
- *Wachtwoord*
- *Voornaam*
- *Achternaam*
- *Bedrijfsnaam*
- *Locatie*
- *Code (van locatie)*
- *Emailadres*
- *Adres*
- *Land*
- *Telefoonnummer*
- *Relatienummer*

Klantgegevens:

- *Bedrijfsnaam*
- *Locatie*
- *Code (van locatie)*
- *Voornaam*
- *Achternaam*
- *Verkorte naam (b.v. roepnaam)*
- *Datum start dienstverband*
- *Datum einde dienstverband*
- *Uurloon inclusief werkgeverslasten*
- *Contracturen per maand*