Versie 1.7

Verwerkersovereenkomst

Bestaande uit:

Deel 1: Data Pro Statement
Deel 2: Standaardclausules voor verwerkingen

Deel 1: Data Pro Statement

versie 1.7 (29 oktober 2018): Wijzigingen sinds versie 1.6:
- Aanvulling op 1.8: ontsluiting berichtgeving door Trengo.
- Diverse tekstuele aanpassingen (hebben betrekking op o.a. grammaticale zaken).

1.1. Trengo Data Pro Statement

Trengo (Data Processor)
https://trengo.com
Leidseveer 2
3511 SB
Utrecht, The Netherlands

Voor vragen over ons Data Pro Statement of databescherming kan contact opgenomen worden via: info@trengo.com of +31(0)85 001 3030.

1.2. Wat is een Data Pro Statement?

Dit document is het Data Pro Statement van Trengo en kan aangepast worden om te kunnen voldoen aan de AVG/GDPR wetgeving, die geldt per 25 mei 2018.

De in deze Data Pro Statement omschreven beveiligingsmaatregelen passen wij regelmatig aan en laten wij toetsen om, in het kader van databescherming, steeds voorbereid te zijn en actueel te blijven. Wij houden u graag op de hoogte van nieuwe versies via onze reguliere communicatiekanalen en/of op onze website.

1.3. Waar is de Data Pro Statement op van toepassing?

De Trengo services en diensten zijn de gedeeltes op de website van Trengo dat exclusief voor Opdrachtgever (de klant) van Trengo beschikbaar is, ook wel “het Trengo account” genoemd.

1.4. Wat is Trengo?

Trengo is “Unified messaging”. Opdrachtgever (de klant) heeft toegang tot een multi-channel (team)-inbox met daarin de mogelijkheid voor het koppelen - of synchroniseren van contactkanalen, zoals mail, social messaging (sociale mediakanalen) en spraak-communicatie. Opdrachtgever, tevens de verantwoordelijke, kiest bij bestelling zelf welke services en diensten zoals contactkanalen, dus eventueel ook diensten van derden, hij of zij toevoegt. Zie https://trengo.com/product voor de contactkanalen (channels) en de daarbij behorende uitleg en werking.

1.5. Beoogd gebruik van Trengo.

Trengo is ontworpen en ingericht om gegevens te verwerken en te synchroniseren voor digitaal berichtenverkeer via Social messaging, maar ook via LiveChat, mail en SMS. Daarnaast is Trengo ook geschikt om mee te bellen (telefonie). Verder heeft Trengo een Chatbot die de klant kan helpen met het automatisch beantwoorden van vragen op de diverse contactkanalen en er is een Help Center kanaal. In Trengo bieden wij de Opdrachtgever ook de mogelijkheid om vrije velden aan te maken en op allerlei plaatsen mogelijk vrije notities in te geven. Het is de verantwoordelijkheid van de Opdrachtgever om de inhoud en aard van registratie van deze informatie te controleren en eventueel te minimaliseren.
N.B. Bij en voor het gebruik van Trengo is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Verwerken van deze gegevens met of via de services of diensten door Opdrachtgever (de klant) is ter eigen beoordeling door Opdrachtgever.

1.6. Trengo past privacy by design toe.

Bij het ontwerp van alle Trengo services en diensten is rekening gehouden met privacy. Net zoals bij beveiligingen wordt privacy in elke update behandeld en doorlopend verbeterd. Opdrachtgever en hun gebruikers uploaden, versturen, ontvangen, synchroniseren en verwerken zelf hun gegevens en kunnen zelf deze gegevens en documenten wijzigen. Op verzoek van Opdrachtgever kan Trengo deze gegevens wijzigen en verwijderen op de servers van Trengo.

1.7. Bij Trengo kiest Opdrachtgever zelf of hij Trengo toegang geeft tot zijn Trengo account.

Om de Opdrachtgever beter van dienst te kunnen zijn (ook bij supportvragen), kan een geselecteerd aantal Trengo supportmedewerkers, die een Trengo geheimhoudingsverklaring hebben getekend, alleen en uitsluitend op verzoek van Opdrachtgever of hun gebruikers bij de gegevens en de accountinstellingen. Dit is alleen mogelijk, indien in het Trengo account van Opdrachtgever, de instelling “Ja, ik geef het Trengo-team toegang tot mijn account voor ondersteuning” is aangevinkt. Alleen een eigenaar (beheerder) van het Trengo account heeft toegang tot “dat vinkje” via https://web.trengo.eu/admin/company_profile.

1.8. Trengo verwerkt persoonsgegevens binnen en soms buiten de EU/EER.

Opdrachtgever (de Trengo klant) kan diensten en/of accounts van derden, zoals Facebook Messenger,

Twitter, Telegram en andere sociale media koppelen en/of synchroniseren via Trengo contactkanalen. Belangrijk om te weten is dat deze of andere derden mogelijk data buiten de EU/EER verwerken. Het is aan Opdrachtgever ter eigen beoordeling of deze derden voldoen aan de door Opdrachtgever gestelde eisen. Deze derden zijn geen Trengo Sub-Processors en -Contractors (Subverwerkers). Opdrachtgever, tevens de verantwoordelijke, heeft zelf een (verwerkers)overeenkomst met deze derden gesloten en kiest ook zelf welke diensten en accounts hij/zij wel of niet koppelt en/of synchroniseert met het Trengo account. Trengo heeft geen invloed op - en neemt geen verantwoordelijkheid voor het verwerken van data (waaronder persoonsgevens) door de sociale mediakanalen, die middels de te koppelen respectievelijke sociale mediakanalen aangeleverd wordt c.q. gekoppeld en/of gesynchroniseerd wordt in Trengo door Opdrachtgever op verzoek van laatstgenoemde.

Trengo ontsluit slechts data (waaronder mogelijk persoonsgevens) via alle mogelijke kanalen die er gekoppeld kunnen worden aan Trengo en is derhalve niet verantwoordelijk voor de acties en/of verwerkingen die derde partij(en) gedaan hebben, doen en mogelijk kunnen doen met deze data vóórdat deze door Trengo ontsloten wordt, ontsloten werd en mogelijk ontsloten kan worden. Indien deze derde partij(en) niet voldoen aan de door Opdrachtgever gestelde eisen, adviseren wij de Opdrachtgever géén gebruik te maken van deze diensten en deze niet te koppelen en/of synchroniseren met Trengo. Wij verwijzen Opdrachtgever(s) graag naar de privacyovereenkomsten van die derde partij(en) aangaande het verwerken van data (waaronder mogelijk persoonsgevens) door deze derde partij(en).

1.9. Trengo Sub-Processors en -Contractors (Subverwerkers)

Trengo werkt samen met Sub-Processors en -Contractors voor het ondersteunen voor het beheren, beveiligen, monitoren en optimaliseren van de data op onze servers. De hosting van onze servers gebeurt bijvoorbeeld bij een provider welke ISO 27001, ISO 9001, PCI-DSS, NEN 7510 en ISAE 3402 Type I is gecertificeerd. Deze organisaties ondergaan een strenge selectieprocedure, zodat we zeker weten dat ze de vereiste technische expertise hebben en het juiste niveau van beveiliging en privacy kunnen bieden en garanderen. Daarnaast hebben wij ook een Trengo Checklist voor beveiligingsmaatregelen Sub-Processors en -Contractors. Indien de Trengo klant dat wenst, verstrekken wij op verzoek meer informatie over deze Sub-Processors en -Contractors en hoe deze door ons gebruikt worden en in welke situatie(s).

Subprocessors - infrastructuur en dataopslag

Bedrijf	**Omschrijving**	**Vestigingsland**
Tilaa B.V.	Cloud Service Provider	Nederland
Amazon, Inc.	Cloud Service Provider	United States
Google, Inc.	Cloud Service Provider	United States
TransIP	Cloud Service Provider	Nederland

Subcontractors

Lemonbit	Verantwoordelijk voor het beheer, de optimalisatie, de beveiliging, en de infrastructuur.

Subprocessors - dienstspecifiek

Bedrijf	**Omschrijving**
MessageBird B.V.	Verwerking van SMS.
Spryng B.V.	Verwerking van SMS.
Mailgun	Verwerking van e-mail.
Mandrill	Verwerking van e-mail.
Twilio	Verwerking van VoIP
Onesignal	Verwerking van multiplatform pushberichten.
Algolia, Inc.	Verwerking van zoekaanvragen.
Pusher, Ltd.	Real-time dataverwerking.

N.B. Bij sommige Subprocessors kunnen wij helaas niet kiezen in welk datacentrum de gegevens verwerkt worden, zoals bijvoorbeeld de mailverwerking van Mailgun. Wij proberen het gebruik van dat soort diensten te minimaliseren en zorgen er altijd voor dat de partner met wie we samenwerken aangesloten is bij het Privacy Shield Framework.
Het is aan Opdrachtgever (de Trengo klant) ter eigen beoordeling of deze Sub-Processors en -Contractors voldoen aan hun eisen. Zo NIET, adviseren wij de opdrachtgever GEEN gebruik te maken van de Trengo diensten. Wij adviseren in die situatie Opdrachtgever om contact met ons op te nemen voor meer informatie.

1.10. Trengo ondersteunt haar Opdrachtgever

In het geval dat een betrokkene een verzoek tot inzage, zoals bedoeld in artikel 35 Wbp, of een verzoek tot verbetering, aanvulling, wijziging of afscherming, zoals bedoeld in artikel 36 Wbp, richt aan Trengo, zal Trengo het verzoek doorsturen aan de verantwoordelijke Opdrachtgever en zal deze het verzoek verder afhandelen. Trengo mag de betrokkene daarvan op de hoogte stellen.

1.11. Beëindiging van de overeenkomst met Opdrachtgever

Na beëindiging van de overeenkomst met Opdrachtgever, verwijdert Trengo de gegevens die hij voor Opdrachtgever heeft verwerkt uiterlijk binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn. Alleen en uitsluitend op schriftelijk verzoek van Opdrachtgever kan deze periode worden verlengd.

1.12. Beveiligingsbeleid

Technische en organisatorische maatregelen
Trengo heeft voldoende technische en organisatorische maatregelen genomen met betrekking tot de te verrichten verwerkingen van persoonsgegevens, tegen verlies of tegen enige vorm van onrechtmatige

verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens). Zoals logische toegangscontrole voor het gebouw en kantoor, gebruik makend van persoonsgebonden toegangspasjes, verificatie door personeel en camerasystemen. De data is redundant opgeslagen bij onze Sub-Processor Tilaa, welke ISO (27001, ISO 9001, PCI-DSS, NEN 7510, ISAE 3402 Type I) gecertificeerd is. Er is beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie en is door Sub-Processor Tilaa een 24/7 SLA aangeboden. Het beheer van onze servers is alleen via bepaalde IP adressen te benaderen. Wij hebben steekproefsgewijze controle op naleving van het beleid met behulp van een Trengo Checklist voor beveiligingsmaatregelen. Uiteraard kijkende naar de stand van de techniek, de gevoeligheid van de persoonsgegevens en de aan het treffen van de beveiliging verbonden kosten, gebruiken wij encryptie (versleuteling) van digitale bestanden. Alleen na overleg staan wij toe dat Verantwoordelijke audits (bijv. een penetration test) laat uitvoeren om vast te stellen of aan alle beveiligingseisen wordt voldaan. Vulnerability en penetration tests zijn o.a. gedaan door BELRON Group Risk & Assurance (vulnerability/penetration) te Londen. Relevante en noodzakelijke data van Verantwoordelijke kan in gangbaar formaat geëxporteerd worden vanuit Trengo via de API

N.B. Opdrachtgever stelt alleen persoonsgegevens aan Trengo ter beschikking voor verwerking indien zij zich ervan heeft verzekerd dat de vereiste beveiligingsmaatregelen zijn getroffen.

1.13 Datalekprotocol

In geval van een datalek
Indien Trengo een datalek ontdekt, zal Trengo Opdrachtgever (de klant) zo snel mogelijk, maar uiterlijk binnen 24 uur, telefonisch op de hoogte stellen. Daarnaast zal er ook een mail naar de beheerder van het Trengo account worden verstuurd, met daarin de volgende informatie:

1. Soort incident.
2. Samenvatting van het incident.
3. Indien bekend en het incident plaatsvond bij een subverwerker, de naam van de subverwerker.
4. Indien bekend het minimaal tot maximaal aantal hoeveelheid personen die betrokken zijn.
5. Indien bekend de omschrijving van de groep mensen die betrokken is bij de inbreuk.
6. Datum inbreuk, indien bekend tussen (begindatum) en (einddatum), of nog niet bekend.
7. Aard van de inbreuk zoals Lezen, Kopiëren, Veranderen, Verwijderen, Vernietigen, Diefstal, Nog niet bekend, of Anders.
8. Indien bekend om welk type persoonsgegevens het gaat zoals, Telefoonnummers, E-mailadressen of andere adressen voor elektronische communicatie, Toegangs- of identificatiegegevens, Financiële gegevens, of Onbekend.
9. Indien bekend welke gevolgen de inbreuk kan hebben voor de persoonlijke levenssfeer van de betrokkenen.
10. Daarnaast zullen wij omschrijven welke technische en organisatorische maatregelen zijn getroffen om de inbreuk op te lossen en om verdere inbreuken te voorkomen.

Data Processor zal Opdrachtgever (de klant) desgewenst ondersteunen bij het meldproces aan de Autoriteit Persoonsgegevens in Nederland. Nadrukkelijk geven wij aan dat het wel of niet melden altijd de verantwoordelijkheid blijft van Opdrachtgever.

N.B. Indien Data Processor een actief lek ontdekt, zal deze om schade te voorkomen, eventueel zonder overleg met de beheerder van het Trengo account (Verantwoordelijke) en indien mogelijk, direct worden gestopt. Het stoppen van het actieve datalek kan gebeuren door het blokkeren van bepaalde of alle gebruikersaccounts, het verplaatsen van data naar een veilige locatie, het uitschakelen van het systeem, het isoleren van een indringer van buitenaf, het aanpassen van firewall-configuraties, het wijzigen van beheer- en onderhoudswachtwoorden, het installeren van afleidingssystemen en/of zelfs het tijdelijk stopzetten van de (web)diensten. Indien het Trengo-team onvoldoende in staat is om het lek onder controle te krijgen, schakelen wij professionele hulp in.

1.14 Audits en controle op dit Data Pro Statement

Opdrachtgever heeft het recht om periodiek audits uit te (laten) voeren om te controleren of wij voldoen aan dit Data Pro Statment en de beveiliging van onze systemen. We spannen ons altijd in om aan dit statement te voldoen. Het kan zijn dat we ons door een auditor laten controleren en dus zelf audits laten uitvoeren. Als dit het geval is, kan Opdrachtgever altijd de rapportage bij ons op kantoor inzien. Alleen als Opdrachtgever met goede en feitelijk onderbouwde argumenten kan aantonen dat we ons niet aan ons Data Pro Statement houden, dan heeft Opdrachtgever het recht om zelf een audit uit te laten voeren door een externe auditor op eigen kosten. Dit recht heeft Opdrachtgever ook als we nog geen auditrapport ter inzage hebben liggen. Als Opdrachtgever een audit wilt (laten) uitvoeren, kondigt hij dit minimaal -14- dagen van tevoren schriftelijk aan ons aan. Komt de datum en/of het tijdstip van de audit ons, ongeacht de reden, niet uit, dan laten we dit aan opdrachtgever weten en doen we een voorstel voor een vervangende datum en/of tijdstip. De personen die de externe audits uitvoeren, houden zich aan de beveiligingsprocedures die bij Trengo van kracht zijn. Dat betekent, bijvoorbeeld, dat ze geheimhouding afspreken. De personen die de audit uitvoeren, de organisatie die de audit uitvoert en Opdrachtgever houden de uitslag van de audit geheim. Het is niet toegestaan hierover met derden te communiceren. Dit mag wel als we hiervoor nadrukkelijk schriftelijk toestemming hebben gegeven. We overleggen dan hier graag eerst met Opdrachtgever over. Voldoet de externe auditor niet aan onze kwaliteitseisen, dan behouden we het recht voor om deze te weigeren.

Deel 2: Standaardclausules voor verwerking

Deel 2 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.

2.1. Definities

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

1. Autoriteit Persoonsgegevens (AP): toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 Avg.
2. Avg: de Algemene verordening gegevensbescherming.
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.

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.
5. Data subject (betrokkene): een geïdentificeerde of identificeerbare natuurlijke persoon.
6. Opdrachtgever: partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.
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.
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.
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.

2.2. Algemeen

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

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.
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.

2.3. Beveiliging

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.
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. 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.
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.
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.
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.

2.4. Inbreuken in verband met persoonsgegevens

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 zo snel mogelijk, zonder onredelijk vertraging maar uiterlijk binnen 24 uur, informeren via de mail en indien mogelijk ook op het telefoonnummer van de beheerder van het Trengo account. Opdrachtgever zorgt er zelf voor dat mailadres en telefoonnummer bereikbaar zijn, functioneren en up-to-date zijn. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens. 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 aan 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.

2. 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.
3. Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever. Data Processor zal de Opdrachtgever om goedkeuring vragen voor aanvullende opdrachten. Data Processor zal een schatting van de maximale kosten geven, inclusief benodigde uurtarieven à € 120,-. Goedkeuring van Opdrachtgever wordt gevraagd in geval van voorspelde overschrijding van de maximale kosten.

2.5. Geheimhouding

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

2.6. Looptijd en beëindiging

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.
2. Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige

nieuwe of nadere overeenkomst tussen partijen.

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.
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.
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.

2.7. Rechten data subjects, data protection impact assessment (DPIA) en auditrechten

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.
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.
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.
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.

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.
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.

2.8. Subverwerkers

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

2.9. Overig

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