

Verwerkersovereenkomst Softmakers B.V.

Versie: 2.0 / 1 januari 2022

Bestaande uit:
Deel 1. Data Pro Statement
Deel 2. Standaardclausules voor verwerkingen

Deel 1: Data Pro Statement

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor 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):

Softmakers B.V., Orteliuslaan 850 te Utrecht

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met de volgende contactpersonen:

- H. Th van der Steen, email huibvandersteen@softmakers.nl, telefoon +31 35 5828183
- W.E.W. Troost, email: wilcotroost@softmakers.nl, telefoon: +31 35 5828183

2. Dit Data Pro Statement geldt vanaf 1 januari 2022, versie 2.0

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 dienst van Softmakers

Tim Software-as-a-Service (SAAS) / ook aangeduid als TimWeb.

4. Omschrijving Tim

Tim is een universeel cloud informatiesysteem voor mkb en non-profit organisaties ter ondersteuning van de informatiebehoefte, communicatie en werkprocessen.

5. Beoogd gebruik van Tim

Tim is geschikt voor het vastleggen van database gegevens, (Office365) documenten en zakelijke conversaties zoals email. In samenwerking met de opdrachtgever wordt gedefiniëerd welke informatie moet worden vastgelegd en of er sprake is van uitwisseling van informatie met externe systemen.

Uitsluitend indien de opdrachtgever hier uitdrukkelijk voor kiest wordt 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 Tim door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. Softmakers heeft bij het ontwerpen van Tim privacy by design op de volgende wijze toegepast:

Als onderdeel van de verplichte implementatieprocedure wordt samen met de opdrachtgever een specifieke indeling gekozen voor de vast te leggen informatie.

Indien het privacy gevoelige informatie betreft zal Softmakers hier expliciet melding van maken aan de opdrachtgever en informeren naar de noodzaak voor het vastleggen van deze informatie.

Softmakers controleert de gegevens niet en zal gegevens alleen inzien op verzoek van de klant, bijvoorbeeld als dat nodig is om een vraag aan de helpdesk te beantwoorden.

De opdrachtgever beslist welke gegevens hij wil vastleggen en aanvaard daarmee de verantwoordelijkheid voor het gebruik ervan door zijn organisatie.

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

8. Softmakers verwerkt alle Tim informatie waaronder de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.

9. Softmakers maakt gebruik van de volgende sub-processors (sub-verwerkers):

- **TransIP** : hosting van de database systemen binnen de EU/EER (<https://www.transip.nl/legal-and-security/certificeringen/>)
- **Microsoft** : documenten en emails worden vastgelegd in een specifieke Office365 OneDrive die door de opdrachtgever zelf wordt afgenomen bij Microsoft. De opdrachtgever dient hiervoor (als onderdeel van zijn bedrijfsbrede gebruik van Office365) een separate Verwerkersovereenkomst met Microsoft te sluiten. Het is voor Nederlandse afnemers gebruikelijk dat de Office365 gegevens in EU/EER worden vastgelegd.
- **Ekco** : EU/EER lokatie voor encrypted backup (<https://www.ek.co/nl/home/over-ekco/partners-en-certificeringen/>)

10. Softmakers ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:

Hiertoe geauthoriseerde medewerkers van opdrachtgever kunnen te allen tijde inloggen en zelf gegevens exporteren, aanpassen of verwijderen.

Opdrachtgever kan via de helpdesk een ticket aanmaken met verzoeken om een bijzondere export, aanpassing of verwijdering van gegevens.

11. Softmakers zal op de volgende wijze medewerking verlenen aan Data Privacy Impact Assessments:

Opdrachtgever kan via de helpdesk een ticket aanmaken met een verzoek voor assistentie bij een DPIA onderzoek.

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

13. Na beëindiging van de Overeenkomst met opdrachtgever retourneert Softmakers alle persoonsgegevens die voor opdrachtgever zijn verwerkt binnen 3 maanden op de volgende manier:

Een recente backup van de volledige database met gegevens van de opdrachtgever wordt op zijn OneDrive geplaatst.

Beveiligingsbeleid

14. Softmakers heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van Tim:

De Tim databases met informatie zijn ondergebracht bij een ISO/IEC 27001:2013 gecertificeerde hosting provider en zijn voor slechts een beperkt aantal medewerkers van Softmakers toegankelijk voor onderhoudswerkzaamheden via een dedicated firewall. Alle andere toegang tot de gegevens in de database is uitsluitend mogelijk via de TimAPI op basis van een voorafgaand authenticatie- en autorisatieproces.

De Tim applicatie zelf draait in de browser van de gebruiker en wisselt uitsluitend informatie uit met de TimAPI middels met HTTPS (TLS 1.2) encryptie beveiligde verbindingen.

Toegang tot de Tim applicatie voor gebruikers van de opdrachtgever wordt verleend op basis van een Single SignOn (SSO) protocol. Authenticatie vindt plaats middels de Active Directory die ook als basis dient voor de Office 365 omgeving van de klant. De inrichting, het toezicht en het onderhoud van deze Active Directory valt geheel onder de verantwoordelijkheid van de opdrachtgever. Medewerkers van Softmakers kunnen niet beschikken over de (persoonlijke) aanmeldgegevens van de Tim gebruikers.

De functionaliteit en toegang tot de informatie in Tim (autorisatie) vindt plaats op basis van functiegroepen. De opdrachtgever bepaalt welke functiegroepen benodigd zijn en welke gebruikers daar lid van zijn.

Softmakers draagt dagelijks na 02:00 zorg voor een offsite backup van de database gegevens. Het transport naar de backup lokatie vindt plaats via een TLS 1.2 verbinding en de informatie wordt bij de bron AES 256 bit, CBC encrypted. De encryptiesleutels zijn uitsluitend in bezit van Softmakers zodat een backup in geen geval door anderen kan worden ingezien. De dagelijkse backup heeft een retentie van 80 dagen.

Naast de dagelijkse backup vindt er een wekelijkse on-site backup plaats van de database informatie met een retentie van 365 dagen. Deze backup wordt op het systeem bij TransIP geplaatst.

Iedere 4 uur wordt er een snapshot backup gemaakt van de operationele systemen voor disaster recovery doeleinden. Deze backup wordt op het systeem bij TransIP geplaatst.

De klant is zelf verantwoordelijk voor de backup van de bestanden die met Tim worden vastgelegd op zijn Office365 OneDrive.

Datalekprotocol

In geval er toch iets mis gaat, hanteert data processor het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:

15. Definitie datalek

Er is sprake van een datalek als er een inbreuk op de beveiliging plaatsvindt die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot opgeslagen of anderszins verwerkte gegevens.

16. Interne verantwoordelijken melding datalekken

Softmakers BV heeft interne verantwoordelijken voor de verwerking van datalekken aangesteld, die verantwoordelijk zijn voor de melding van een datalek:

- H. Th van der Steen, email huibvandersteen@softmakers.nl, telefoon +31 35 5828183
- W.E.W. Troost, email: wilcotroost@softmakers.nl, telefoon: +31 35 5828183

17. Melding bij ontdekking van een datalek

Degene die een datalek bij Softmakers BV ontdekt, meldt dit per omgaande aan de interne verantwoordelijke

Als een klant een datalek ontdekt, belt deze direct de Softmakers verantwoordelijke

Indien mogelijk, zorgt degene die het datalek heeft ontdekt er gelijktijdig voor dat de gelekte gegevens meteen op afstand worden gewist of ontoegankelijk worden gemaakt

18. Onderzoek door de interne verantwoordelijke

De interne verantwoordelijke onderzoekt onder meer:

- Of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden
- Wie binnen de organisatie betrokken zijn bij het datalek
- Of er een sub-verwerker betrokken is bij het incident
- Welke betrokkende (klanten) zijn geraakt door het incident

19. Bestrijding datalek

De interne verantwoordelijke stopt het datalek indien dat nog kan en neemt voorts de noodzakelijke maatregelen om het datalek zo goed mogelijk te bestrijden.

20. Vaststelling van de gevolgen van een datalek

De interne verantwoordelijke onderzoekt de mogelijke gevolgen van het datalek aan de hand van de aard en de omvang van de gegevens die gelekt zijn en stelt vast wat de nadelige gevolgen voor de klant(en) kan zijn.

21. Medewerking verstrekking gegevens omtrent het datalek

De ontdekker/melder van het datalek biedt alle medewerking aan de interne verantwoordelijke door zo snel en zo goed mogelijk (schriftelijk) antwoord te geven op de volgende vragen:

- Wat is er gebeurd? (omschrijving van het incident)
- Ging het per ongeluk of is het veroorzaakt door kwade opzet (denk aan gehackte gegevens)?
- Wanneer is het gebeurd? (datum en tijdstip)
- Wanneer is het ontdekt en door wie?
- Wat voor gegevens zijn gelekt?
- Zijn de gegevens versleuteld, en zo ja hoe?
- Konden de gegevens op afstand worden gewist of ontoegankelijk gemaakt en zo ja, is dat gebeurd?
- Wat zijn de mogelijke gevolgen voor de klanten van Softmakers?
- Welke klanten zijn hierdoor getroffen?
- Hoeveel personen zijn hierdoor (bij benadering) getroffen?
- Konden er al technische en/of organisatorische maatregelen worden getroffen naar aanleiding van het incident?

22. Beschikbaarheid personeel na ontdekking datalek

De verantwoordelijke van de afdeling vanuit waar het datalek heeft plaatsgevonden alsook de ontdekker van het datalek en iedereen die vanuit hun functie of kennis in staat is om organisatorische en of technische maatregelen te treffen om de gevolgen van het datalek te beperken, houden zich de 1e 24 uur na ontdekking van het datalek beschikbaar voor overleg met de interne verantwoordelijke c.q. eventueel door hem aangewezen experts en voor het zo nodig uitvoeren van opgedragen werkzaamheden als gevolg van het datalek.

23. Beslissing melding datalekken

De interne verantwoordelijke beslist zo spoedig mogelijk doch in elk geval binnen 24 uur na ontdekking van het datalek - al dan niet in overleg met de verantwoordelijke van de afdeling vanuit waar het datalek is ontdekt en of door hem aangewezen experts - of het datalek dient te worden gemeld aan de klant(en).

Een datalek wordt in principe altijd gemeld aan de klanten, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen

De melding van het datalek gaat gepaard met beantwoording van de vragen zoals omschreven in onderdeel "Medewerking verstrekking gegevens omtrent het datalek"

24. Melding datalekken aan de klant

De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de klanten.

Melding geschiedt zo spoedig mogelijk na de ontdekking en uiterlijk binnen 24 uur na ontdekking van het datalek aan de betreffende klanten

25. Gevolgen melding datalekken

Indien het datalek negatieve gevolgen heeft voor de klanten, dan doet de interne verantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken

Afhankelijk van de aard en de omvang van het datalek voor klanten bepaalt de interne verantwoordelijke:

- op welke wijze klanten worden geïnformeerd (waaronder in ieder geval de mededelingen worden gedaan welke soorten persoonsgegevens getroffen zijn, wat de mogelijke gevolgen zijn, welke maatregelen Softmakers BV neemt en op welke wijze klanten zelf de schade kunnen voorkomen of beperken)
- welke nazorg klanten krijgen .
- welke acties in het belang van de klanten noodzakelijk zijn

26. Bijhouden register datalekken

- De interne verantwoordelijke houdt een register bij van alle datalekken, waarin alle gegevens rondom het datalek worden geregistreerd, zoals:
- Een omschrijving van het incident
- Datum en tijdstip van het datalek
- Datum en tijdstip ontdekking van het datalek
- Ontdekker van het datalek
- Omschrijving van de soort gelekte persoonsgegevens
- Omschrijving aantal betrokkenen per klant.
- Of het incident is gemeld aan de klanten met datum en tijdstip melding
- Op welke wijze klanten zijn geïnformeerd
- De gevolgen van het datalek, met indien mogelijk vermelding van datum en tijdstip
- Welke technische en of organisatorische maatregelen zijn getroffen na ontdekking van het datalek met vermelding van datum en tijdstip

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):** 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, 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 inaccessible), 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

- 9.1. 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.