



NLdigital

Versie: 1.0 – 21 augustus 2026

Verwerkers- overeenkomst

Anura Digital Agency

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):

Anura Digital Agency
Industrieweg 14
9781 AC Bedum

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
info@anurawebdevelopment.nl

2. Dit Data Pro Statement geldt vanaf 21 augustus 2026; en betreft versie 1

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 en kan worden opgevraagd via info@anurawebdevelopment.nl

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor

- Websites & webshops
- Webapplicaties
- Onderhoud aan websites, webshops en webapplicaties
- Hosting, domein & E-mail
- Digitale creatie
- Narrowcasting

‘In de Overeenkomst tussen Data Processor en opdrachtgever is bepaald welke producten/diensten bij Data Processor zijn afgenomen.’

4. Omschrijving product(en)/dienst(en)

- Het ontwerpen, ontwikkelen en opleveren van websites & webshops
- Het ontwikkelen van specifieke maatwerk webapplicaties ter ondersteuning van bedrijfsprocessen van de opdrachtgever.
- Het uitvoeren van technisch onderhoud, het doorvoeren van updates, het oplossen van bugs en het optimaliseren van de werking en beveiliging van de webapplicaties, websites & webshops.
- Het faciliteren van de technische infrastructuur voor het online beschikbaar stellen van websites en webapplicaties, inclusief het beheer van domeinnamen en e-mail hosting/routing.
- Het creëren en beheren van digitale content, visuals en contentdistributie voor digitale informatieschermen narrowcasting en marketingdoeleinden.

5. Beoogd gebruik

Product/dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

Het product/de dienst is ontworpen en ingericht voor het verwerken van reguliere persoonsgegevens die noodzakelijk zijn voor het functioneren van de geleverde digitale oplossingen en de bijbehorende hosting/infrastructuur.

Hieronder vallen onder meer:

- Inzendingen via formulieren en interactieve elementen: Gegevens die door eindgebruikers worden ingevoerd op websites, webshops of applicaties (zoals contactformulieren, offerte-aanvragen, inschrijvingen, reacties of bestelformulieren).
- Gebruikers- en accountgegevens: Gegevens benodigd voor accountbeheer, authenticatie en autorisatie binnen CMS-systemen, webapplicaties en e-mailvoorzieningen.
- Communicatie- en communicatie-inhoud: De inhoud en metadata van e-mailverkeer, systeemnotificaties en berichten die via de gehoste e-mailinfrastructuur of applicaties worden verzonden of ontvangen.
- Klant- en transactiegegevens: Inhoudelijke gegevens rondom bestellingen, facturatie- en leveringsadressen binnen e-commerce omgevingen.
- Systeem- en loggegevens: Technische gegevens zoals IP-adressen, browser- / apparaatgegevens en inloghistorie ter behoeve van beveiliging, performance en foutoplossing (logging).

Afbaking (Bijzondere persoonsgegevens)

- De producten en diensten zijn in beginsel niet standaard ingericht voor het verwerken van bijzondere en/of gevoelige persoonsgegevens of verwerkingen waarvoor specifieke extra beveiligingscertificeringen vereist zijn.
- Indien de opdrachtgever besluit om bijzondere of aanvullende categorieën persoonsgegevens via de diensten/producten te verwerken, dient dit vooraf expliciet schriftelijk te worden overeengekomen en vastgelegd in de overeenkomst of een aanvullende verwerkersovereenkomst, zodat passende (aanvullende) beveiligingsmaatregelen getroffen kunnen worden.

6. Privacy by design/privacy by default

Anura Digital Agency streeft ernaar om de principes van 'Privacy by design' en 'Privacy by default' waar mogelijk en toepasbaar mee te nemen bij het ontwerp, de ontwikkeling en het beheer van haar producten en diensten.

Onze werkwijze en uitgangspunten:

- Inspanningsverplichting: Anura Digital Agency houdt bij het adviseren, bouwen en beheren van digitale oplossingen zoveel mogelijk rekening met privacyvriendelijke instellingen en beveiligingsstandaarden (zoals het gebruik van SSL/HTTPS-verbindingen en het veilig opslaan van inloggegevens).
- Praktische afweging: Waar mogelijk adviseren wij opdrachtgevers over het beperken van de uitvraag van persoonsgegevens (dataminimalisatie) en het instellen van passende autorisaties.

Verdeling van verantwoordelijkheid:

- De opdrachtgever bepaalt uiteindelijk de functionaliteiten, de uit te vragen gegevens, de inzet van cookies of koppelingen van derden, en de bewaartermijnen binnen de applicaties of websites.
- Anura Digital Agency bouwt en configureert de oplossingen primair op basis van de wensen, instructies en specificaties van de opdrachtgever.

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

8. **Data processor verwerkt de persoonsgegevens (gedeeltelijk) buiten de EU/EER. De data processor heeft op de volgende manier geborgd dat een passend beschermingsniveau van toepassing is:**

Toelichting op de gegevensverwerking en locatie:

- Primaire opslag & hosting: De primaire infrastructuur, databases en servers van Anura Digital Agency bevinden zich volledig in Nederland (via TransIP).
- Koppelingen van derden (APIs/Integraties): Voor specifieke functionaliteiten en op instructie of verzoek van de Opdrachtgever kan er gebruik worden gemaakt van (optionele) externe diensten waarvan de leverancier buiten de EU/EER is gevestigd. Denk hierbij bijvoorbeeld aan:
 - Mailtrap: E-mail monitoring binnen specifieke webapplicaties.
 - Google (o.a. reCAPTCHA, Analytics): Voor beveiligings- en geanonimiseerde/statistische doeleinden.
- Plug-ins en uitbreidingen door opdrachtgever: Indien de opdrachtgever zelfstandig (Wordpress-) plug-ins, scripts of koppelingen van derden toevoegt aan de website of applicatie, valt de eventuele doorgifte van persoonsgegevens via deze componenten onder de directe verantwoordelijkheid van de opdrachtgever.

9. **Data processor maakt gebruik van de volgende sub-processors:**

Anura Digital Agency maakt voor de uitvoering van haar diensten gebruik van de onderstaande primaire sub-processor(s):

Sub-processor	Dienst / Doel	Locatie verwerking	Geborgd bescherming
TransIP B.V.	Hosting, VPS, databases & e-mailinfrastructuur	Nederland (EU)	Verwerkersovereenkomst (EU-regelgeving)

Aanvullende en projectspecifieke sub-processors:

Afhankelijk van de specifieke dienstverlening, gekozen functionaliteiten of koppelingen (zoals e-mailtesting, analytics of e-mailmarketing) kan Anura Digital Agency gebruikmaken van aanvullende sub-processors.

Een actuele en volledige lijst van al onze sub-processors, inclusief hun verwerkingslocatie en de bijbehorende waarborgen voor doorgifte, is te raadplegen via:

<https://anurawebdevelopment.nl/verwerkersovereenkomst/subverwerkers/>

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**

Anura Digital Agency ondersteunt de opdrachtgever bij het afhandelen van verzoeken van betrokkenen (zoals het recht op inzage, correctie, verwijdering en dataportabiliteit) op de volgende wijze:

Inzage, correctie en verwijdering:

- Zelfservice via beheersystemen: De door Anura Digital Agency geleverde oplossingen (zoals CMS- en webshopomgevingen) bieden de opdrachtgever in de regel de mogelijkheid om zelfstandig persoonsgegevens in te zien, aan te passen of te verwijderen.

- Technisch maatwerk & ondersteuning: Indien een verzoek niet zelfstandig via de beheersinterface kan worden uitgevoerd (bijvoorbeeld bij gegevens in databases, back-ups of logbestanden), kan de opdrachtgever hiervoor een supportaanvraag indienen bij Anura Digital Agency. Anura Digital Agency voert de gewenste actie op instructie van de opdrachtgever uit.

Dataportabiliteit (gegevensoverdraagbaarheid):

- Anura Digital Agency faciliteert de opdrachtgever door, op verzoek en tegen vergoeding van de geldende tarieven, beschikbare persoonsgegevens in een gestructureerd, gangbaar en machinaal leesbaar formaat (zoals JSON, CSV of XML) te exporteren en aan te leveren.

Doorsturen van verzoeken:

- Indien een betrokken eindgebruiker rechtstreeks een AVG-verzoek bij Anura Digital Agency indient, zal Anura Digital Agency dit verzoek zo snel mogelijk doorsturen naar de opdrachtgever, aangezien de opdrachtgever de verwerkingsverantwoordelijke is.

11. **Data processor zal op de volgende wijze medewerking verlenen aan Data Protection Impact Assessments (DPIA):**

Indien de opdrachtgever op grond van de geldende privacywetgeving (AVG) verplicht is om een Data Protection Impact Assessment (DPIA) of een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens uit te voeren, zal Anura Digital Agency hieraan redelijke medewerking verlenen.

Onze ondersteuning bestaat uit het volgende:

- Het op redelijk verzoek aanleveren van relevante technische en organisatorische informatie over de werking, beveiliging, architectuur en gegevensverwerking van de geleverde producten en diensten.
- De Opdrachtgever dient een verzoek tot medewerking schriftelijk in te dienen bij Anura Digital Agency, vergezeld van de specifieke vragen of onderdelen waarvoor technische expertise benodigd is.
- Omdat het uitvoeren van of meewerken aan een DPIA niet valt onder de reguliere dienstverlening of het standaard onderhoud, worden de werkzaamheden die Anura Digital Agency hiervoor verricht op basis van nacalculatie tegen het geldende uurtarief aan de opdrachtgever doorberekend, tenzij schriftelijk anders is overeengekomen.

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

13. **Retourneren van persoonsgegevens na beëindiging van de Overeenkomst**

Na beëindiging van de overeenkomst zal Anura Digital Agency, naar keuze van de opdrachtgever, alle aanwezige persoonsgegevens en bestanden retourneren of definitief wissen, tenzij een wettelijke bewaarplicht het bewaren hiervan vereist.

- Indien de opdrachtgever hierom verzoekt, worden de gegevens in een gangbaar, digitaal formaat (zoals een database-dump, CSV of ZIP-bestand) eenmalig beschikbaar gesteld. Eventuele

aanvullende werkzaamheden voor de migratie of export worden verricht op basis van nacalculatie tegen het geldende uurtarief.

- Indien geen verzoek tot retournering wordt ingediend, of nadat de export succesvol is overgedragen, worden de persoonsgegevens, applicaties en back-ups binnen uiterlijk 3 maanden definitief van de servers en systemen van Anura Digital Agency verwijderd.

Beveiligingsbeleid

14. Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:

Anura Digital Agency heeft passende technische en organisatorische maatregelen genomen om persoonsgegevens te beschermen tegen verlies, ongeoorloofde toegang of enige vorm van onrechtmatige verwerking:

Pseudonimisering & versleuteling (Encryption):

- Het uitgangspunt is dat alle dataverkeer tussen gebruikers, webapplicaties en servers versleuteld plaatsvindt via SSL/TLS-certificaten (HTTPS).
- At rest (opslag): Gevoelige gegevens zoals wachtwoorden worden altijd versleuteld opgeslagen door middel van hashing. Waar mogelijk en technisch relevant voor de toepassing worden aanvullende persoonsgegevens gehasht of gepseudonimiseerd opgeslagen.

Vertrouwelijkheid & interne Maatregelen:

- Toegangsbeheer & Authenticatie: Twee-factor-authenticatie (2FA) is verplicht op interne systemen van Anura Digital Agency en voor beheerdersaccounts met uitgebreide rechten. Wij passen waar mogelijk zo veel mogelijk 2FA toe.
- Netwerkbeveiliging & Fysieke toegang: Beheer (zoals SSH-toegang) is uitsluitend mogelijk vanaf geautoriseerde werkplekken/IP-adressen op kantoor. Standaardpoorten worden waar mogelijk aangepast. Het kantoor netwerk is gescheiden georganiseerd ten opzichte van andere pandgebruikers.
- Fysieke & Organisatorische richtlijnen: Beleid voor de veilige omgang met hardware (zoals verplicht 'locken' bij het verlaten van de werkplek) en het niet delen van netwerksleutels.

Integriteit & beschikbaarheid (Server & applicatiebeveiliging):

- De VPS-infrastructuur bevat actieve firewalls, brute-force protection en geautomatiseerde periodieke malware-scanning.
- Applicatiebeveiliging bij WordPress: Inzet van gespecialiseerde beveiligingsplugins indien gevraagd door de opdrachtgever met actieve firewall-bescherming, inlogbeveiliging en het afdwingen van sterke wachtwoorden.
- Risico's worden gemonitord (onder andere via CVE-meldingen). Bij bekende kwetsbaarheden worden direct definitieve of tijdelijke patches doorgevoerd op servers, websites en plug-ins.

Herstel bij incidenten:

- Er worden periodiek back-ups gemaakt die zowel intern als op een gescheiden omgeving worden opgeslagen en tot 30 dagen worden bewaard.

- Continuous monitoring van de beschikbaarheid van de websites en webapplicaties indien door opdrachtgever aangevraagd.
15. **Data processor heeft zich geconformeerd aan een Information Security Management System (ISMS), geborgd in/via:**
Geen formeel ISMS; wij hanteren een intern beveiligingsbeleid dat we periodiek controleren en bijstellen.
16. **Data processor heeft de volgende verificaties en certificeringen:**
- Geen

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:**

Anura Digital Agency hanteert een vast protocol bij mogelijke beveiligingsincidenten en datalekken:

- Welke incidenten: Incidenten waarbij sprake is van ongeoorloofde toegang tot, verlies of wijziging van persoonsgegevens (of een reëel risico daartoe).
- Meldtermijn: Onverwijld, uiterlijk binnen 48 uur na ontdekking.
- Wijze van melden: Per e-mail of telefonisch aan de vaste contactpersoon van de Opdrachtgever.
- Inhoud van de melding: De melding bevat informatie over de aard van het incident, de getroffen gegevens, de verwachte gevolgen en de genomen herstelmaatregelen.
- Samenwerking: Anura Digital Agency ondersteunt de opdrachtgever bij het verdere onderzoek en herstel.

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):** 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

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.