Versie: v1.0 | 1 januari 2025

Verwerkers-overeenkomst

SC Workforce

Management Systems BV

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):**
   SC Workforce Management Systems BV, Maanlander 47, 3824 MN Amersfoort
   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met onze Data Protection Officer, via security@atrea.nl.

2. **Dit Data Pro Statement**
   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 communicatiekanalen.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor: Atrea van SC Workforce Management Systems BV.**

4. **(Functionele) omschrijving Atrea oplossing**

   Atrea Tijdregistratie

   Aan- en afwezigheidsregistratie en verlofregistratie zijn standaard onderdelen van onze tijdregistratie software. Hierdoor profiteren werkgevers en medewerkers van de inzichten die tijd je kan geven. Inzichten in gewerkte uren, toeslagen en verlofuren zijn niet alleen bepalend voor werkroosters of bezettingsplanningen, het zorgt ook voor minder gedoe in de salarisadministratie en verstevigt de vertrouwensband tussen medewerker en werkgever.

   Atrea Toegangscontrole

   Goede toegangscontrole is essentieel voor bedrijven. Het is de manier om te voorkomen dat ongewenste personen jouw organisatie binnen komen. Maar ook de methode om diefstal door eigen personeel te voorkomen. Met de toegangscontrole van Atrea krijg je:

   - Real-time inzicht in de locatie van medewerkers
   - Toegangscontrole voor bezoekers
   - Toegang beperken tot verschillende gebieden op basis van o.a. tijdstip, persoon en afdeling.
   - Historisch inzicht in wie, wanneer een gebied binnen is gekomen.

   Gebruik je toegangscontrole gecombineerd met tijdregistratie van Atrea? Dan krijg je nog meer.

   - Toegangscontrole gekoppeld aan werkroosters.
   - Automatisch inklokken bij ontgrendelen van de deur.

   Atrea Activiteitenregistratie (projecten-, kostenplaats- en orderregistratie)

   Met projectregistratie geef je een verdiepingsslag op jouw tijdregistratie. Met tijdregistratie software weet je de “wie” en “wanneer”. Met projectregistratie weet je ook de “wat”.
   Kostenplaatsregistratie software geeft je inzicht in de gewerkte uren per kostenplaats. Voorbeelden van kostenplaatsen zijn afdelingen, productielijnen, ruimtes en machines. Daarnaast zorgt de software voor

duidelijkheid richting medewerkers, doordat ze voor de start van de werkdag weten waar ze moeten werken.
Wanneer je werkt op basis van orders is het interessant om een verdiepingsslag te maken op jouw tijdregistratie. Zodat je weet wie aan welke order heeft gewerkt en hoeveel tijd daar aan is besteed.

Atrea Bezoekersregistratie

De beveiliging van je pand is belangrijk. Naast ongewenst bezoek en werknemers heb je nog één derde categorie: bezoekers. Met de module bezoekersregistratie weet jij precies wie er bij je op bezoek is en zorg je ervoor dat ze alleen op plekken kunnen komen waarvoor ze toegestaan zijn.

Samengevat biedt Atrea een compleet personeelsregistratiesysteem waarmee klanten werktijden (aanwezigheid), ziekte- en vakantieverlof (afwezigheid), toegangscontrole, personeelsplanning en roostering op 1 centrale plek kunnen bijhouden en optimaliseren. Atrea helpt klanten tijd, moeite en kosten te besparen door (onder andere) verzoeken om vakantieverlof te verwerken, personeelsleden te lokaliseren, toegang te autoriseren op basis van werkroosters en projectbeheer te vergemakkelijken.

5. **Beoogd gebruik**

De Atrea oplossing is ontworpen en ingericht om er de volgende soort gegevens mee te werken:

a. Persoonlijke gegevens zoals naam, geboortedatum etc.
b. Contactgegevens zoals adres, e-mailadres, telefoonnummer, etc.
c. Burgerlijke staat en informatie over partner en kinderen
d. Officiele gegevens en screeninggegevens zoals paspoort/ID, Verklaring omtrent het Gedrag (VOG), strafrechtelijke veroordelingen, strafbare feiten, etc
e. Betalingsgegevens, inclusief bankrekeningnummer
f. Nummer werknemer (medewerkersnummer)
g. Functie-omschrijving
h. Contractgegevens inclusief maar niet beperkt tot brutosalaris, vergoedingen en andere personeelsbeloningen.
i. Werkgerelateerde uitgaven
j. Tijdregistratie, aan- en afwezigheidsinformatie, toegangsinformatie, activiteiteninformatie, etc
k. Kwalificaties, inclusief cv en referenties
l. Informatie over onderwijs, opleiding, etc.
m. Informatie over persoonlijke ontwikkeling en evaluaties
n. Verificatiegegevens om de services te gebruiken, zoals gebruikersnaam, IP-adres, pc-naam, enz.
o. Activiteiten uitgevoerd door klantgebruikers bij het gebruik van de diensten

6. **Data processor heeft bij het ontwerpen van het product/de dienst privacy by design/privacy by default op de volgende wijze toegepast:**

a. Gegevensminimalisatie: Het ontwerp van de Atrea oplossing is gebaseerd op het verzamelen van zo min mogelijk persoonlijke gegevens die nodig zijn voor het beoogde doel. Dit minimaliseert het risico op gegevensinbreuken en beschermt de privacy van gebruikers.
b. Pseudonimisering: Indien mogelijk zijn persoonlijke gegevens geanonimiseerd of gepseudonimiseerd voordat ze verder worden verwerkt. Dit minimaliseert het risico op identificatie van individuen en beschermt hun privacy.

c. Standaardinstellingen voor privacy: de Atrea oplossing is zo ontworpen dat de standaardinstellingen de hoogste mate van privacy bieden. Waar mogelijk bieden wij de gebruikers de mogelijkheid actief in te stemmen met het delen van meer persoonlijke informatie, in plaats van dit standaard te delen.

d. Transparantie en gebruikerscontrole: Het ontwerp van de Atrea oplossing omvat duidelijke communicatie over hoe persoonlijke gegevens worden verzameld, gebruikt en gedeeld. Gebruikers hebben ook controle over hun gegevens, inclusief de mogelijkheid om deze te wijzigen of te verwijderen.

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

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

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

Atrea kan, afhankelijk van de gekozen dienst, gebruikmaken van de diensten van de volgende sub-verwerker:

Sub-verwerker	**Doel**	**Binnen of buiten EU/EER**
Hosted.nl	Fysieke hosting	Binnen
Mailjet	Verzending e-mails en rapportages	Binnen
Google Firebase	Verzending notificaties mobiele applicatie	Binnen
Equinix	Datacenter Rackspace & Hosting activiteiten voor Atrea Mobile Middleware	Binnen

10. **Data processor verleent medewerking aan Data Privacy Impact Assessments.**
Hiervoor worden kosten in rekening gebracht tegen de dan geldende standaard uurtarieven.

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

Beveiligingsbeleid / dataprotectiebeleid

12. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
Atrea en haar sub-processoren hebben de volgende veiligheidsmaatregelen ingevoerd om haar product of dienst te beschermen :

Technische beveiligingsmaatregelen	**Organisatorische beveiligingsmaatregelen**
Encryptie en privacy-vriendelijke instellingen zijn standaard geimplementeerd. Encryptie instellingen zijn standaard geimplementeerd op server niveau.	Atrea heeft zich geconformeerd aan het volgende beheersysteem voor informatiebeveiliging (ISMS) : ISO 27001. Certificaat afgegeven door een onafhankelijke deskundige partij.

Een autorisatiemodel (rechten en rollen) dat volledig kan worden ingericht naar de eigen wensen van de klant.	Atrea heeft een gedragscode ingevoerd.
De mogelijkheid om het gebruik af te dwingen van sterke wachtwoorden binnen de applicatie en via groepsbeleid.	Atrea heeft een interne procedure ingevoerd voor de melding van inbreuken op gegevens en gegevensincidenten.
Pseudonimisering wanneer Atrea Persoonsgegevens intern verwerkt. Dit proces houdt in dat identificerende gegevens van personen worden vervangen door kunstmatige identificatoren (pseudoniemen), waardoor de gegevens zonder aanvullende informatie niet meer aan specifieke individuen kunnen worden gekoppeld.	Vertrouwelijkheidsverplichtingen in arbeidsovereenkomsten, ingehuurd personeel of ander personeel dat toegang heeft tot Persoonsgegevens die worden verwerkt onder de verantwoordelijkheid van de klant en de Gegevensverwerkers' verantwoordelijkheid
Toezicht op de goede werking van websites en gerelateerde API's.	Logische toegangscontrole door middel van kennis, zoals een wachtwoord of persoonlijke toegangscodes.
Atrea beveiligt haar systemen en netwerken met firewalls en antivirussoftware.	Fysieke toegangscontrole zoals beveiligingspassen.
Verplichte encryptie van dataverkeer via HTTPS	Jaarlijkse bewustmakingsopleiding voor werknemers inzake informatiebeveiliging
Atrea gebruikt en implementeert meerfactor authenticatie (MFA) om de beveiliging van zowel haar eigen diensten als die van externe partijen te versterken. Dit houdt in dat gebruikers bij het inloggen meerdere vormen van verificatie moeten doorlopen, zoals een wachtwoord gecombineerd met een eenmalige code die via een authenticator-app wordt verstuurd. Dit verhoogt de beveiliging aanzienlijk door een extra laag bescherming toe te voegen naast het traditionele wachtwoord.	
Daarnaast adviseert Atrea Single Sign-On (SSO), wat gebruikers in staat stelt om met één set inloggegevens toegang te krijgen tot meerdere applicaties en diensten. Dit vereenvoudigt het inlogproces voor gebruikers	

en vermindert het aantal keren dat zij hun wachtwoord moeten invoeren, terwijl het tegelijkertijd de beveiliging en beheerbaarheid van toegangsrechten verbetert.	

13. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):** ISO 27001

14. **Data processor heeft de volgende certificeringen:** ISO 27001

Datalekprotocol

15. **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:**
Voor het geval er toch iets misgaat, heeft Atrea het volgende protocol voor datalekken vastgesteld om ervoor te zorgen dat de klant wordt geinformeerd over incidenten:
Er is een procedure voor het intern melden van incidenten. Indien Atrea binnen haar organisatie een datalek ontdekt, zal Atrea de klant hierover zo spoedig mogelijk informeren. Atrea zal zoveel mogelijk relevante informatie overleggen, waaronder een beschrijving van het incident, de aard van de inbreuk, de aard van de Persoonsgegevens of de betrokken categorieen van Betrokkenen. Indien mogelijk zal de klant binnen 24 uur op de hoogte worden gebracht. Atrea zal als verwerker voor haar klanten geen melding doen aan het College Bescherming Persoonsgegevens (AP) of aan Betrokkenen; het al dan niet geen melding wordt gedaan is en blijft de verantwoordelijkheid van de klant. Indien gewenst zal Atrea de klant bijstaan tijdens het meldingsproces. De dienstdoende Data Protection Officer (DPO) behandelt alle mededelingen namens Atrea. Onze DPO kan gecontacteerd worden via e-mail op : security@atrea.nl

Afsluiting

16. De verwerkingen die u als klant van Atrea (of elk ander systeem van toegangscontrole, tijdsregistratie of activiteitenregistratie) gaat uitvoeren, worden door de Autoriteit Persoonsgegevens gezien als een personeelvolgsyteem. Dit betekent dat uw privacybeleid daarop moet zijn ingericht en dat u, indien er een OR is, deze verwerking ter goedkeuring aan de OR moet worden voorgelegd. Wij adviseren u hiermee rekening te houden bij de implementatie van Atrea of een ander personeelvolgsysteem.

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):** toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 Avg.

1.2 **Avg:** de Algemene verordening gegevensbescherming.

1.3 **Data Processor**: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.

1.4 **Data Pro Statement**: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, sub-processors, datalekken, certificeringen en omgang met rechten van Data subjects.

1.5 **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon.

1.6 **Opdrachtgever:** partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.

1.7 **Overeenkomst**: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.

1.8 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.

1.9 **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 Avg.

Artikel 2. Algemeen

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.

2.2 Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.

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

2.4 Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de Avg, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de Avg en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de Avg zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de Avg voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de Avg handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor.

Artikel 3. Beveiliging

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico's en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten of door de overheid uitgegeven persoonsnummers.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde

beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

Artikel 4. Inbreuken in verband met Persoonsgegevens

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 Avg) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

4.2 Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 Avg moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 Avg.

4.4 Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

Artikel 5. Geheimhouding

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

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

Artikel 6. Looptijd en beëindiging

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

6.2 Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn

verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (***render inaccessable***), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen aan Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de Avg is ten aanzien van de Persoonsgegevens.

Artikel 7. Rechten Data subjects, Data Protection Impact Assessment (DPIA) en Auditrechten

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 Avg.

7.3 Data Processor zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

7.4 Data Processor kan desgewenst de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of een daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige, indien hij over een dergelijk certificaat of auditrapport beschikt.

7.5 Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de Avg of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.6 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn

product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.7 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

Artikel 8. Sub-Processors

8.1 Data Processor heeft in het Data Pro Statement vermeld of, en zo ja welke derde partijen (sub-processors of subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere sub-processors in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

8.3 Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

Artikel 9. Overig

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

Heb je vragen?

Onze juristen kunnen je voorzien van advies en ondersteuning. Neem contact met ons op.

NLdigital organiseert ook verschillende juridische workshops en bijeenkomsten. Houd hiervoor de agenda op onze website in de gaten. Leden van NLdigital kunnen hier kosteloos aan deelnemen. Ben je nog geen lid en wil je ook profiteren van deze en vele andere mogelijkheden van het lidmaatschap? Bekijk de voordelen!

NLdigital
De Corridor 5
3621 ZA Breukelen
info@nldigital.nl
+31 (0) 348 - 49 36 36
KVK 3017 4840

NLdigital