Verwerkersovereenkomst

Algemene verordening gegevensbescherming

LOGICVISION

Deel I: Data Pro Statement
Deel II: Standaardclausules voor verwerkingen

Document info:

Document	: Verwerkersovereenkomst Logic Vision Dynamics producten - Avg
Versie	: 1 mei 2018
Auteur	: F. Verpalen

DEEL I: 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

Logic Vision B.V.
Hakgriend 18B
3371 KA Hardinxveld-Giessendam
Nederland

Tel: +31 (0)184-677588
info@logicvision.nl
www.logicvision.nl
KVK: 29051064
BTW: NL8079.94.066.B01
ING: 67.77.17.105
BIC: INGBNL2A
IBAN: NL05INGB0677717105

Hierna tevens te noemen: ***Data Processor***

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met de kwaliteitscoördinator of IT consultant van Logic Vision. Te bereiken via het algemene nummer.

2. Dit Data Pro Statement geldt vanaf 1 mei 2018

De in dit Data Pro Statement omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze normale kanalen.

3. Dit Data Pro Statement is van toepassing op de door Data Processor geleverde producten en diensten

4. Omschrijving product

Microsoft Dynamics is een flexibele bedrijfsmanagement- en CRM oplossing. Het stroomlijnt de primaire bedrijfsprocessen en faciliteert medewerkers in het uitvoeren van goed relatiebeheer. Hiervoor zijn een aantal specifieke Logic Vision add-ons ontwikkeld, waaronder FuelVision en TugVision. Voor meer informatie over Dynamics producten of diverse add-ons, zie onze website: https://www.logicvision.nl/nl/softwareproducten/microsoft-dynamics-nav en https://www.logicvision.nl/nl/softwareproducten/microsoft-dynamics-365-for-sales.

5. Beoogd gebruik

De door Data Processor geleverde producten zijn ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

Gegevens met betrekking tot:

- Financieel beheer en accounting: geldbeheer, assets en bankzaken.
- CRM: contactbeheer, taken, verkoopkansen.
- Projectbeheer: schattingen, volgen van projecten en het beheren van de capaciteit.
- Toeleveringsketen, productie en bedrijfsprocessen: volgen en beheren van productie, voorraad, bestellingen en leveranciers.
- HRM: (basis) personeelsbestand.

- Relatiebeheer: klanten, accounts, contactpersonen.
- Leadbeheer bij potentiele klanten.
- Registratie van verkoopkansen.
- Onderhoud: abonnementen, service.
- Communicatie: campagnes, nieuwsbrieven e.d.

Omdat het standaard HRM onderdeel binnen bijvoorbeeld Microsoft Dynamics NAV o.a. beschikt over de mogelijkheid om een afwezigheidsregistratie en lidmaatschap vakbond bij te houden, betekent dit dat Microsoft Dynamics NAV geschikt is om bijzondere gegevens te verwerken. De genomen extra beveiligingsmaatregelen worden verder omschreven in punt 12. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door Opdrachtgever is ter eigen beoordeling door Opdrachtgever.

6. **Data Processor gebruikt de Data Pro Standaardclausules voor verwerkingen, welke in deel II van dit document te vinden zijn.**

7. **Data Processor verwerkt de persoonsgegevens van zijn Opdrachtgever binnen de EU/EER.**

Indien Data Processor voor ontwikkeldoeleinden beschikt over een kopie van uw database staat deze in een door Data Processor beveiligde omgeving. Daarnaast staat de database op de locatie waar Opdrachtgever zelf hun database hebben opgeslagen, on premise dan wel in een (private) cloud. Bij het gebruik van een cloudoplossing worden de gegevens opgeslagen in de regio waar het hoofdkantoor van de organisatie is gevestigd.
Zie https://www.microsoft.com/online/legal/v2/?docid=25. Indien u dus in Europa bent gevestigd, worden de persoonsgegevens in de EU verwerkt.

8. **Indien gegevens buiten de EU/EER verwerkt worden: de Data Processor heeft op de volgende manier geborgd dat een passend beschermingsniveau van toepassing is:**

Indien van toepassing kunnen deze gegevens separaat ter hand worden gesteld.

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

Wij maken op dit moment geen gebruik van sub-processors, tenzij data processor de hosting voor u doet.

10. **Data Processor ondersteunt Opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**

Voor zover redelijkerwijs mogelijk en met inachtneming van de aard van de verwerking zal Data Processor de Opdrachtgever ondersteunen in het verwerken (lezen, verwijderen of aanpassen) van gegevens in de database die bij Opdrachtgever is opgeslagen. Data Processor heeft hierbij het recht om eventuele kosten bij Opdrachtgever in rekening te brengen. Extraheren van gegevens geschiedt in .csv of .xml format.

11. **Na beëindiging van de overeenkomst met een Opdrachtgever verwijdert 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).**

BEVEILIGINGSBELEID

12. Data Processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:

Fysieke toegangscontrole (gebouw/ kantoor/ datacenter)

- Automatische toegangscontrole.
- Veiligheidssloten.
- Sleutelbeheer (sleutel uitgifte etc.)
- Bezoekersregistratie.
- Bewegingsmelders.
- Camera toegangsbewaking.
- Alarmsysteem.
- Een gedocumenteerde toegangscontrole voor datacenters en serverruimten. Toegang alleen voor bevoegde personen, naam- en sleutelnummer wordt geregistreerd.

Toegangscontrole tot systemen (systemen/ computers/ servers/ randapparatuur)

- Medewerkers hebben een geheimhoudingsverklaring ondertekend.
- Role & Access management (toewijzen van individuele gebruikersrechten).
- Toewijzen van individuele gebruikersnamen en wachtwoorden.
- Authenticatie d.m.v. gebruiksnaam en wachtwoord.
- Minimumeisen aan samenstelling wachtwoorden.
- Aparte gebruiksrechten voor ICT-systemen.
- Gebruik van VPN-software.
- Centraal beheer van smartphones (met mogelijkheid om remote data te wissen).
- Gebruik van disk encryptie bij laptops/ notebooks.
- Gebruik van softwarematige firewall (gebruikerssystemen)
- Implementatie van firewalls.

Integriteitscontrole (systemen/ computers/ servers/ randapparatuur)

- Wachtwoorden hebben minimale complexiteit.
- Systemen maken gebruik van antivirus software.
- Gebruik van Web-Applicatie-Firewall (WAF).
- Logfiles worden periodiek bekeken.
- Gedocumenteerde procedure voor melden beveiligingsincidenten. (Zie punt 15).

Toegangscontrole tot data

- Disk encryptie van back-ups en laptops.
- Veilig wissen van media voor hergebruik, afdanking.
- Veilig vernietigen van media bij afdanking.

Beveiliging van gegevens in transit

- Gebruik van VPN verbinding bij gebruik van Wifi.
- Disk encryptie.
- TLS encryptie van alle communicatie (Web-Client, API's, mobile Apps).

Toezicht op invoer van gegevens

- Anonimiseren of pseudonimiseren persoonsgegevens (op aanvraag van Opdrachtgever).

Toezicht op subverwerkers (enkel indien gebruik wordt gemaakt van hosting en/ of SaaS diensten)

- Selectie van (sub)verwerker met inachtneming data security geschiedenis.
- (Sub)verwerker heeft gedocumenteerde procedures m.b.t. de Avg.
- (Sub)verwerker heeft functionaris voor de gegevensbescherming (indien verplicht volgens de Avg)
- Onderzoek naar documentatie en genomen beveiligingsmaatregelen (sub)verwerker.
- Werknemers bij (sub)verwerker hebben geheimhoudingsplicht.
- Vernietiging van data na afloop contract is vastgelegd.
- Periodieke evaluatie door (sub)verwerker genomen maatregelen.
- Afspraken zijn vastgelegd in een (sub)verwerkersovereenkomst met bijbehorende standaardclausules voor verwerking.

Beschikbaarheid

- Stroomvoorziening gegarandeerd door UPS.
- Temperatuur en luchtvochtigheid wordt gemeten in server.
- Brand- en rookmelders.
- Toegangscontrole op serverruimte.
- Periodieke test van terugzetten van back-up.
- Beveiligde opslag van off-site back-ups.
- Airconditioning of koeling in serverruimte.
- Gezekerde stroomvoorziening.

Gescheiden verwerking

- Logische (softwarematige) scheiding van gegevens van klanten.
- Gebruik van aparte OTAP-straat.
- Productiesysteem gescheiden van ontwikkel- test- en acceptatiesysteem.

Overig

- Beperkte toegang tot de door Data Processor geleverde on premise databases. Enkel Consultants en Solution Developers hebben toegang. De beperkte toegang wordt ingeregeld m.b.v. een Rollen- en Rechtencentrum. Wanneer we op locatie bij de Opdrachtgever werken wordt door Opdrachtgever een account met bijbehorende rollen en rechten in de database beschikbaar gesteld.
- Beperkte toegang tot de Dynamics 365 databases omdat door Opdrachtgever voor enkel de betrokken projectleden een account beschikbaar wordt gesteld. Vaak betreft dit de inloggegevens van de administrator gebruiker bij Opdrachtgever.
- Op aanvraag van Opdrachtgever kunnen bijzondere persoonsgegevens (lidmaatschap vakbond, afwezigheidsregistratie) verwijderd of omgezet worden in dummy data indien deze bij Data Processor on premise komen te staan.
- De mogelijkheid om FTP te gebruiken, welke wederom gekoppeld is aan de betreffende gebruiker + wachtwoord. Hierbij kan men enkel bij afgeschermde map (dus niet bij klantgegevens, back ups etc.) Tevens wordt bij elke nieuwe inlog op de ‘gast FTP’ het wachtwoord opnieuw gereset.

13. Data Processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):

Zie beleid zoals omschreven in punt 12.

14. Data Processor heeft de volgende certificeringen:

Data Processor beschikt op dit moment nog niet over een certificering, maar is voornemens zich te laten certificeren door het Data pro certificaat van Nederland ICT zodra dat beschikbaar komt.

DATALEKPROTOCOL

15. In geval er toch iets mis gaat, hanteert Data Processor het volgende datalekprotocol om ervoor te zorgen dat opdrachtgevers op de hoogte zijn van incidenten:

Een beveiligingsincident is een gebeurtenis waardoor **mogelijk een datalek kan ontstaan**. Er is dus nog niet geconstateerd dat er daadwerkelijk een datalek heeft plaatsgevonden. Enkele voorbeelden:

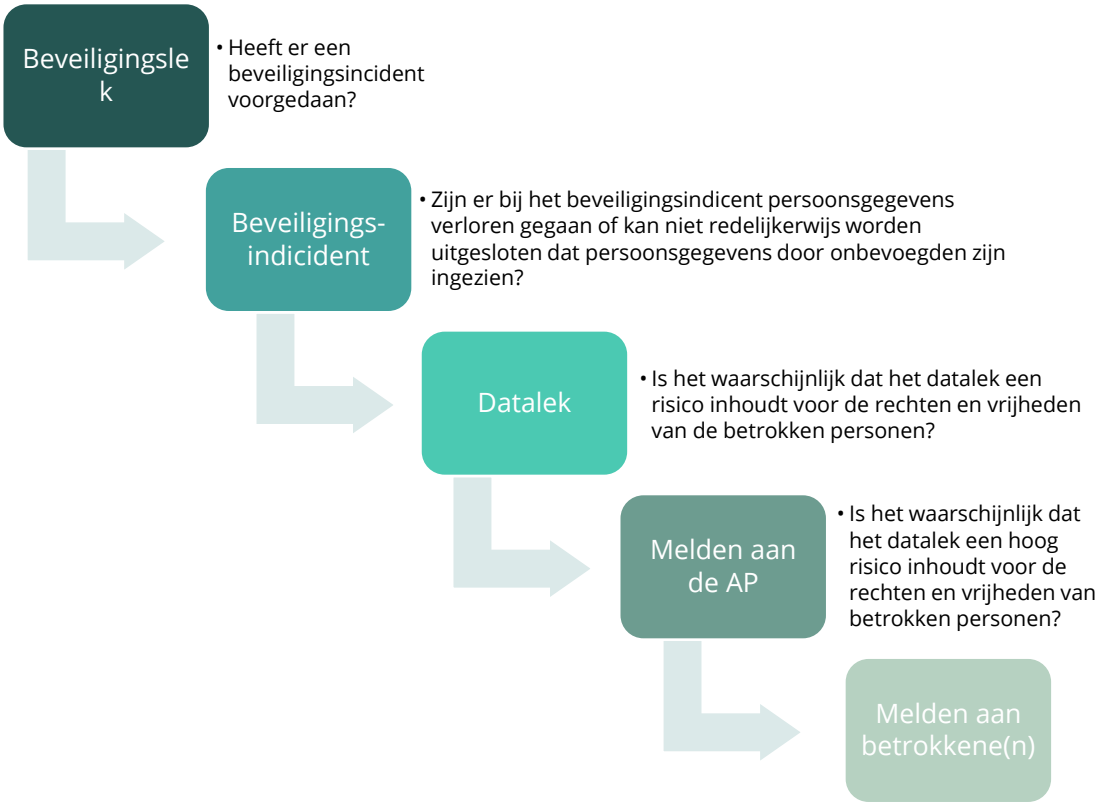
- Een kwijtgeraakte/gestolen usb stick, smartphone, tablet of laptop.
- Een inbraak door een hacker.
- Een calamiteit in een datacentrum of server ruimte.

Als blijkt dat er bij het beveiligingsincident **persoonsgegevens verloren zijn gegaan**, of niet redelijkerwijs kan worden uitgesloten dat persoonsgegevens **door onbevoegden zijn ingezien** (=verwerkt). Voorbeelden zijn:

- Een kwijtgeraakte/gestolen usb stick, smartphone, tablet of laptop waarbij de toegang niet goed is beveiligd met een wachtwoord/ code.
- Waarbij de toegang wel goed is geblokkeerd en dus niet toegankelijk, maar waarbij er geen back up is van de data op het device.
- Een technische storing waarbij onbevoegden toegang hebben tot persoonsgegevens.
- Het verstrekken van toegang tot persoonsgegevens aan niet-geautoriseerde personen. Uit een logbestand blijkt dat de niet geautoriseerde persoon inderdaad inzage heeft gehad in deze persoonsgegevens.
- Een poststuk met daarin persoonsgegevens welke niet op de (juiste) eindbestemming is bezorgd.
- Een hack waarbij data (bijvoorbeeld gebruikersnamen en wachtwoorden) zijn ontvreemd.
- Informatie met persoonsgegevens op papier welke in de prullenbak is achtergelaten en door een derde (onbevoegde persoon) eruit is gehaald.
- Een calamiteit in een datacentrum/serverruimte waarbij data verloren is gegaan en er géén recente back up is.
- Een e-mail met daarin een bijlage met persoonsgegevens die aan een verkeerde persoon is verstuurd.
- Verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn (dus niet in de BCC).
- Een malware besmetting (als je op en hyperlink hebt geklikt in een phishing mail en deze niet tijdig hebt ontdekt en gemeld bij ICT).

Data Processor heeft in het kader van het melden van beveiligingsincidenten de volgende maatregelen getroffen:

1. Indien het datalek bij de Data Processor heeft plaatsgevonden, dan meldt Data Processor dit zonder onredelijke vertraging aan de Opdrachtgever.
2. De Opdrachtgever inventariseert het risico van het datalek.
    - Als het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokken personen, dan hoeft de melding niet aan de AP te worden gemeld.
    - Als het datalek wel een risico inhoudt voor de betrokkenen, dan meldt de Opdrachtgever dit uiterlijk binnen 72 uur aan de AP.
    - Indien het datalek ook een hoog risico voor inhoudt voor de betrokkenen, dan informeert de Opdrachtgever de betrokkene(n).



Data Processor zal bij het doen van zijn melding aan Opdrachtgever de volgende afspraken in acht nemen:

De melding (per e-mail) bevat de volgende gegevens

- Onderwerp: <Melding datalek> gericht aan de projectverantwoordelijke van de Opdrachtgever.
- Datum melding en de datum waarop Data Processor op de hoogte is geraakt van het beveiligingsincident.
- Samenvatting van het beveiligingsincident.
- Op welke beveiligingsmaatregel heeft zich een beveiligingsincident voorgedaan?
- Op welke manier heeft het beveiligingsincident zich voorgedaan? Oftewel, wat is de aard van het beveiligingsincident? Gaat het om lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens?
- Wat is de oorzaak van het beveiligingsincident?
- Indien bekend:
    - Omschrijving van de groep mensen van wie Persoonsgegevens zijn betrokken bij het beveiligingsincident.
    - Aantal personen getroffen door het beveiligingsincident.
    - Type Persoonsgegevens (om wat voor Persoonsgegevens gaat het? Namen, toegangs- of identificatiegegevens, financiële gegevens, bijzondere gegevens etc.)
- Voorgestelde of genomen maatregelen om het datalek aan te pakken c.q. ter beperking van eventuele nadelige gevolgen.

Informatie mag zonder onredelijke vertraging in stappen worden verstrekt aan de AP.

Documentatieplicht

Opdrachtgever is verantwoordelijk om alle datalekken te documenteren. Deze documentatie omvat ten minste:

- Feiten omtrent gemelde datalek.
- Gevolgen.
- Corrigerende maatregelen.

DEEL II: STANDAARDCLAUSULES VOOR VERWERKINGEN

Versie: januari 2018 Nederland ICT

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, subverwerkers, datalekken, certificeringen en omgang met rechten van Data subjects.

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

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

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

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

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

ARTIKEL 2 ALGEMEEN

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

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

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

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

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

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

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

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Data Processor.

ARTIKEL 3 BEVEILIGING

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

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

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

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

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

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

ARTIKEL 4 INBREUKEN IN VERBAND MET PERSOONSGEGEVENS

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

is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

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

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

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

ARTIKEL 5 GEHEIMHOUDING

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

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

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

ARTIKEL 6 LOOPTIJD EN BEËINDIGING

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

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

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen Opdrachtgever.

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

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

ARTIKEL 7 RECHTEN DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENT (DPIA) EN AUDITRECHTEN

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

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

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

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

7.5 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

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

ARTIKEL 8 SUBVERWERKERS

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

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

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

ARTIKEL 9 OVERIG

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