

Versie: 07-2023

Verwerkers- overeenkomst KPI Solutions B.V.

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):

KPI Solutions B.V.
Oranjesingel 2
6511 NS Nijmegen
KVK: 66116619

Voor vragen over dit Data Pro Statement of dataproductie kan contact opgenomen worden met:

Ralph Fransen
Partner
ralph@kpisolutions.nl
+31 85 2735879

2. Dit Data Pro Statement geldt vanaf 11 juli 2023, versie 07-2023:

Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van dataproductie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze website. U vindt de nieuwste versie altijd op <https://kpisolutions.nl/overige-voorwaarden/>

In versie 07-2023 is er een toevoeging gedaan over specifieke kaartvisualisaties voor Microsoft Power BI, in artikel 13.

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

- a Template- en maatwerkrapportages
- b KPI Connectoren
- c Opzetten, inrichten en hosten van een datawarehouse
- d Apps en Automatiseringen
- e Machine learning en AI
- f Training, bedrijfsadvies en consultancy

4. Omschrijving “Template- en maatwerkrapportages”:

Templaterapportages zijn gestandaardiseerde Power BI rapportages die de klant voor een eenmalig bedrag of een maandelijkse fee kan afnemen. Maatwerkrapportages worden voor de klant ontwikkeld, volledig nieuw of vanuit de basis van een templatereportage. Voor de beschikbaarstelling van een template-, maatwerk- of elke andere vorm van rapportage, wordt data opgehaald, getransformeerd en geladen in datasets in Microsoft Power BI Service. Vervolgens wordt het rapport gepubliceerd binnen de Office 365-omgeving van KPI Solutions, waarbij de klant inloggegevens ontvangt, of de omgeving van de klant. Voor het ontwikkelen en beheren van rapportages wordt de data daarnaast gebruikt in Microsoft-software zoals Power BI Desktop en Excel op lokale machines. Er kan in overleg met de klant ook aanvullende data worden opgeslagen op producten/diensten van Microsoft. Ontwikkelde rapportages worden daarnaast opgeslagen op producten/diensten van Microsoft zoals SharePoint.

5. Omschrijving “KPI Connectoren”:

De 'KPI Connector' maakt verbinding met application programming interfaces (API's), portals, bestandssystemen, databases of vergelijkbare gegevensbronnen waar de ontvanger inloginformatie of connectie-informatie toegang toe geeft. De gevraagde data wordt vervolgens op het Microsoft Azure platform verwerkt en in een door KPI Solutions beheerde Microsoft Azure database gerepliceerd. Deze database (ook 'datawarehouse' genoemd) valt onder het product KPI Connector. Vanuit de betreffende database zijn de gegevens te bereiken en te gebruiken voor de klant of voor gebruik in rapportages. Voor het ontwikkelen en beheren van connectoren wordt de data daarnaast gebruikt in Microsoft-software zoals Visual Studio Code op lokale machines. Bij uitzondering kan worden overeengekomen dat de verwerking plaatsvindt op een door de klant aangewezen locatie buiten de KPI Solutions omgeving of dat de data wordt gerepliceerd naar een door de klant aangewezen database buiten de KPI Solutions omgeving, maar alleen in opdracht van de klant.

6. Omschrijving “Opzetten, inrichten en hosten van een datawarehouse”:

Binnen deze dienst wordt advies gegeven over inrichting van data warehouses en dataverplaatsing. Als hierbij data wordt verwerkt door KPI Solutions, is dit een KPI Connector zoals in dienst B of een Automatisering zoals in dienst D. Daarnaast wordt voor alle KPI Connectoren wordt een inrichtingsstarief gerekend voor de connector en het opzetten van het datawarehouse.

7. Omschrijving “Apps en Automatiseringen”:

Naast de als connectoren verkochte oplossingen, worden ook dataverplaatsing en data-invoeroplossingen op het Microsoft Azure platform en Microsoft Power Platform (Power Apps, Power Automate) op maat aangeboden. Hierbij wordt altijd met de klant de inrichting besproken. Power Apps zijn applicaties die voor de klant worden ontwikkeld. De applicatie wordt gehost op Microsoft Power Platform, binnen de omgeving van de klant. De klant heeft hierbij het beheer over gebruikers, beveiliging en systeeminrichting. Automatiseringen kunnen in verschillende programmeertalen worden ontwikkeld. De data wordt verwerkt op het Microsoft Azure platform en/of het Microsoft Power Platform. Hierbij kan data worden opgehaald, verwerkt, getransformeerd en/of tussen verschillende bronsystemen worden uitgewisseld. Automatiseringen kunnen worden gehost door KPI Solutions of door de klant. Voor het ontwikkelen en beheren van automatiseringen wordt de data daarnaast gebruikt in Microsoft-software zoals Visual Studio Code op lokale machines. Bij uitzondering kan worden overeengekomen dat de verwerking plaatsvindt op een door de klant aangewezen locatie buiten de KPI Solutions omgeving of dat de data wordt gerepliceerd naar een door de klant aangewezen database buiten de KPI Solutions omgeving, maar alleen in opdracht van de klant.

8. Omschrijving “Machine Learning en AI”:

Dataverwerking in kunstmatige intelligentie zoals ‘machine learning’ wordt ontwikkeld in samenspraak met de klant. Voor alle diensten, en dus ook deze dienst, geldt dat alleen gebruik wordt gemaakt van de data van de klant zelf en/of data uit openbare bronnen. Modellen worden dus niet getraind op basis van diverse klanten, maar wordt bij elke klant opnieuw ingesteld om ongewenste informatie-uitwisseling te voorkomen. Kunstmatige intelligentie is een zeer breed vakgebied, waarbij oplossingen zowel door KPI Solutions kunnen worden gehost als door de klant.

9. Omschrijving “Training, bedrijfsadviesing en consultancy”:

Indien KPI Solutions de klant ondersteunt, kan er toegang tot de applicaties en/of databases van de cliënt benodigd zijn bij advisering op basis van de door rapportages gegenereerde inzichten, het datagestuurd werken binnen de organisatie en het gebruik van de aangeboden oplossingen. Als hierbij data wordt gerepliceerd door KPI Solutions, is dit een KPI Connector zoals in dienst B. Als hierbij rapporten worden gepubliceerd, is dit een rapportage zoals in dienst A.

10. Beoogd gebruik - Diensten zijn ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

KPI Solutions richt zich op een breed bedrijfsspectrum, waarbij het uitgangspunt dat alle data die op rapportageniveau interessant is, een commercieel of competitief voordeel oplevert en/of meer inzichten kan genereren wordt aangrepen om Business Intelligence toe te passen. Hierbij stroomt de data van het bronsysteem via de KPI Connector en/of dataverplaatsing en data-invoer oplossingen naar de template- en maatwerkrapportages. Persoonsgegevens worden uiteraard alleen gebruikt voor de dienstverlening aan de betreffende klant zelf.

De daadwerkelijke toegang tot de gegevens is afhankelijk van de rechten die de verwerkingsverantwoordelijke heeft verleend bij het verstrekken van de inloginformatie of connectie-informatie aan de verwerker. KPI Solutions is altijd de verwerker van klantdata, en nooit de verwerkingsverantwoordelijke. KPI Solutions beoordeelt in het kader van de KPI Connector niet de inhoud van de gerepliceerde gegevens, maar stelt zich op als *cloud storage partner*, in de rol van verwerker.

Er is geen 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 het hiervoor omschreven product of dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om deze gegevens niet te laten verwerken of verwerking te accepteren naar beoordeling van de verwerkingsverantwoordelijke. Alle gegevens die KPI Solutions als verwerker verwerkt namens de verwerkingsverantwoordelijke zijn ten allen tijde in te zien door de klant in het datawarehouse.

Persoonsgegevens betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. KPI Solutions verwerkt persoonsgegevens, onder andere maar niet beperkt tot:

- Persoonsnamen van klanten, medewerkers, leveranciers, enz.;
- Aanspreektitels;
- Klantnummers, personeelsnummers, leveranciersnummers, enz.;
- Adressen en IP-adressen;
- Telefoonnummers en emailadressen;
- Zakelijke functies en werkgevers.

11. Data processor heeft bij het ontwerpen van de dienst privacy by design op de volgende wijze

toegepast:

- KPI Solutions beschrijft de dienstverlening als 'cloud centric'. De structurele dataverwerking vindt volledig plaats in de cloud, waarbij alle producten in hetzelfde Microsoft Azure datacentrum binnen de EU/EER wordt gehost. Alleen gedurende de tijdelijke ontwikkelings- en/of beheerswerkzaamheden wordt data lokaal verwerkt en/of bij subverwerker b. en c.;
- Alleen de gegevens die de klant vraagt worden gerepliceerd. De KPI Connectoren verwerken alleen de gegevens die worden gespecificeerd. De BI Rapportages bevatten waar mogelijk alleen de gegevens waarover wordt gerapporteerd. De standaardversies van KPI Connectoren kunnen alleen data lezen vanuit een bronsysteem en plaatsen in een datawarehouse om processen zo simpel mogelijk te houden (zogenaamde 'KISS'-methode);
- KPI Connectoren halen bij elke vernieuwing nieuwe data op, waarbij verwijderde gegevens uit de bronsystemen ook worden verwijderd uit het datawarehouse. Er is dus geen langdurige opslag van gegevens die de verwerkersverantwoordelijke niet meer heeft mogelijk, tenzij dit is overeengekomen in add-ons zoals 'tijdreizen' en 'foto maken';
- KPI Solutions houdt rekening met de OWASP (Open Worldwide Application Security Project®) top 10 kwetsbaarheden, zodat kwetsbaarheden vermeden worden. Door te verwerken vanuit gestructureerde bronsystemen (zoals databases, json, xml, csv) en naar een gestructureerd datawarehouse of doelsysteem worden risico's gemitigeerd;
- Alle databases zijn binnen Microsoft Azure gescheiden opgeslagen. Elke klant heeft intern een bijbehorende Sharepointsite, waarop bestanden zoals rapportages zijn opgeslagen. Elke klant heeft een eigen Power BI werkruimte, waarin rapportages worden gepubliceerd.

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

13. Data processor verwerkt tijdens structurele dataverwerking de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER. Data Processor verwerkt gedurende de tijdelijke ontwikkelings- en/of beheerswerkzaamheden gedeeltelijk buiten de EU/EER. De Data processor heeft op de volgende manier geborgd dat een passend beschermingsniveau van toepassing is:

- Data processor heeft met de partijen in het derde land vastgestelde standaardbepalingen afgesloten volgens uitvoeringsbesluit (EU) 2021/914 van de Europese Commissie;
- Data wordt alleen buiten de EU/EER verwerkt voor de duur van de tijdelijke ontwikkelings- en/of beheerswerkzaamheden en niet voor structurele gegevensverwerking. Nadat de expliciete taak die is gevraagd is voltooid, worden alle gegevens verwijderd door de subprocessor b. en c.;
- Na de tijdelijke ontwikkelings- en/of beheerswerkzaamheden vindt de structurele dataverwerking plaats binnen de EU/EER. Zelfs tijdens deze tijdelijke werkzaamheden wordt data zoveel mogelijk binnen de EU/EER opgeslagen en datagebruik door deze sub-processors geminimaliseerd. Tijdelijke werkzaamheden zijn bijvoorbeeld de ondersteuning in ontwikkeling van rapportages of connectoren door medewerkers van de sub-processor;
- Alle data-opslag en dataverwerking in structurele processen vindt plaats binnen de EU/EER. Structurele processen zijn bijvoorbeeld de periodieke datavernieuwing en geplande rapportagevernieuwingen. Alle datawarehouses, virtuele machines, virtuele netwerken, zijn volledig binnen de EU/EER ingericht. Hierbij verlaat data de EU/EER niet.

- De enige uitzondering op alle voorgaande punten in artikel 13 zijn drie kaartvisuels in Power BI. Deze visuals kunnen gebruikmaken van services die zich buiten de geografische regio, nalevingsgrens of nationale cloudinstantie van de Power BI-tenant bevinden. Deze functies maken gebruik van mappingmogelijkheden die worden geleverd door een derde partij. Microsoft deelt de adres- en locatiequery's met de derde partij, maar niet de naam van de klant of eindgebruiker die de query heeft ingevoerd. Deze visuals worden alleen door KPI Solutions gebruikt op verzoek van de klant en worden altijd getoond in het Power BI-rapport. Gegevens worden nooit gedeeld wanneer deze visuals niet worden gebruikt. Hiervoor gelden de bijbehorende Microsoft-voorwaarden. Als de rapportage wordt gepubliceerd in de omgeving van de klant, zijn deze partijen geen subverwerker meer van KPI Solutions maar direct van de klant.
 - Power BI map and filled map visuals: Microsoft Bing, TomTom and SK Telecom
 - Azure Maps Power BI visual: Microsoft Azure, TomTom
 - ArcGIS Maps visual: Esri

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

- a Microsoft
 - Producten onder andere, maar niet beperkt tot: Azure platform, Power Platform (Power BI, Power Apps, Power Automate), Office 365 (Sharepoint, Windows);
 - Alle data wordt verwerkt binnen de EU/EER.
- b Intellify Solutions Pvt. Ltd.; en
- c N-iX LTD
 - Data-analyse en rapportageontwikkeling en KPI Connector-ontwikkeling voor alle producten;
 - Alleen voor de duur van de tijdelijke ontwikkelings- en/of beheerswerkzaamheden en niet voor structurele dataverwerking. Data wordt in dat specifieke geval tijdelijk verwerkt buiten de EU/EER.
 - Data processor heeft met de partijen in het derde land vastgestelde standaardbepalingen afgesloten volgens uitvoeringsbesluit (EU) 2021/914 van de Europese Commissie.

15. Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt binnen een week op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).

Beveiligingsbeleid

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

- KPI Solutions heeft een informatiemanagementbeleid dat is vastgelegd in het hierna genoemde Information Security Management System (ISMS). Hierin wordt structureel aandacht besteed aan de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Het managementsysteem is ingericht volgens de PDCA-cyclus (Plan Do Check Act) en is ISO 27001 gecertificeerd.
- KPI Solutions heeft een Security Awareness programma bestaande uit bedrijfsbrede sessies, informatiemails en een online Awareness pakket waar periodiek nieuwe modules worden toegevoegd.
- KPI Solutions is AVG-compliant en voldoet aan wettelijke bewaartermijnen. De klant heeft recht op inzage, vergetelheid, rectificatie en aanvulling, dataportabiliteit, beperking van de verwerking, een menselijke blik bij besluiten en bezwaar, voor zover wettelijk verplicht.
- KPI Solutions heeft beleid vastgesteld over medewerkers, middelen, infrastructuur, architectuur, toegang, cryptografie, back-ups, ontwikkeling, incidenten en continuïteit;
- Door de 'cloud centric' structurele dataverwerking kan altijd gebruik worden gemaakt van de nieuwe versies, updates en ontwikkelingen. Er wordt gestreefd om alle systemen over de laatste beveiligingsupdates te laten beschikken. Alle Azure cloudtoegang is alleen mogelijk via het eigen VPN-netwerk zodat ongewenste toegang wordt voorkomen;
- Gegevens zijn *at rest* en *in transit* altijd versleuteld opgeslagen. Er wordt gebruik gemaakt van onder andere IPsec, TDE, WireGuard®, TLS. Details hierover worden bijgehouden in het ISMS.
- Alle laptops worden centraal beheerd in Microsoft Endoint Manager en zijn van afstand leeg te gooien en van updates te voorzien. Rechten en rollen zijn centraal beheerd.

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

KPI Solutions heeft een Information Security Management System waarin alle structuren, middelen, processen en beleidsstukken zijn opgenomen. Hierbij wordt gebruik gemaakt van het PCT Framework van de ProActive Compliance Tool.

18. Data processor heeft de volgende certificeringen:

- KPI Solutions B.V. is door DigiTrust B.V. gecertificeerd voor de norm NEN-EN-ISO/IEC 27001:2017+A11:2020 onder certificaatnummer DGT271721139. Het toepassingsgebied betreft: Het beveiligen van informatie in relatie tot de ontwikkeling en beschikbaarstelling van rapportages; ophalen, repliceren, verwerken en beschikbaar stellen van data; advisering en training. Dit certificaat is geldig tot 19 mei 2025. ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging.

Datalekprotocol

19. 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:

Het datalekprotocol van KPI Solutions is als volgt beschreven:

“Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Ook hierdoor kunnen de betrokken personen namelijk schade leiden. De algemene verordening gegevensbescherming (AVG) het over een ‘inbreuk in verband met persoonsgegevens’. Hiervan is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG).

Op het moment dat de verwerkingsverantwoordelijke kennis heeft genomen van een datalek is zij verplicht om binnen 72 uur melding te doen bij het meldloket datalekken, via een webformulier op de website van de Autoriteit Persoonsgegevens (AP). Het gaat dan onder andere om gevoelige (persoons)gegevens die 'nadelige gevolgen' kunnen hebben voor KPI Solutions, de verwerkersverantwoordelijke of andere betrokkenen.

KPI Solutions stelt de opdrachtgever hiervan zo spoedig mogelijk in kennis, uiterlijk binnen 24 uur na het constateren ervan. Indien er een contactpersoon/meldpunt datalekken bij ons bekend is, wordt deze geïnformeerd. Als deze niet bekend is, wordt uw Functionaris Gegevensbescherming geïnformeerd. Mocht ook die niet bekend zijn, dan informeren we uw operationele aanspreekpunt of zo nodig uw directie. We delen zoveel mogelijk informatie die u van ons nodig heeft. Dit omvat in ieder geval (1) de aard van de inbreuk, (2) de getroffen maatregelen om de negatieve gevolgen van het datalek te beperken, (3) een beschrijving van de geconstateerde en de vermoedelijke gevolgen, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie. De primaire verantwoordelijkheid voor het melden bij de Autoriteit Persoonsgegevens ligt bij de verwerkingsverantwoordelijke. In eerste instantie informeren wij daarom uw contactpersoon.”

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 beveiligd 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 verwerkerovereenkomst 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 verwerkerovereenkomst 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 verwerkerovereenkomst, 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.

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!](#)

KPI Solutions B.V.
Oranjesingel 2 6511 NS Nijmegen
Lange Viestraat 2b, Utrecht

info@kpisolutions.nl
+31 85 2735879