Rijksoverheid

Toelichting bij het gebruik van het Model Verwerkersovereenkomst ARIV

Deze Toelichting is openbaar, maar maakt geen onderdeel uit van de Overeenkomst. Bij twijfel over de betekenis en/of uitleg van de Verwerkersovereenkomst ARIV kan hetgeen in deze Toelichting staat mede bepalend zijn. De Toelichting doet geen afbreuk aan hetgeen partijen in een concreet geval zijn overeengekomen.

I – Inleiding

Als een opdracht wordt verstrekt op basis van de ARIV dan kan daarin besloten liggen dat Leverancier persoonsgegevens moet verwerken ten behoeve van Koper. In dat geval moeten partijen een verwerkersovereenkomst sluiten op grond van art. 28, derde lid, van de Algemene verordening gegevensbescherming (hierna: Verordening). In een verwerkersovereenkomst maken Koper en Leverancier afspraken over de Verwerking van Persoonsgegevens in het kader van de Overeenkomst. De afspraken gaan over de bescherming van de persoonsgegevens van Betrokkenen.

Indien bij de uitvoering van dienstverleningsovereenkomsten Persoonsgegevens worden Verwerkt, dient in beginsel het Model Verwerkersovereenkomst ARIV te worden gebruikt. De Verwerkersovereenkomst is dan een bijlage bij de in het kader van de opdracht te sluiten Overeenkomst.

Dit model is opgesteld aan de hand van artikel 28 van de Verordening. Bij de formulering van de artikelen is zoveel mogelijk aangesloten bij de tekst van de Verordening. Daar waar niet de letterlijke tekst van de Verordening is gevolgd, houdt dit verband met nationale wet- en regelgeving of de inhoud van de Overeenkomst / ARIV. Zo worden Partijen in dit model aangeduid als Koper en Leverancier en niet als verwerkingsverantwoordelijke en verwerker. In de overwegingen wordt geëxpliciteerd dat Koper kwalificeert als verwerkingsverantwoordelijke in de zin van artikel 4, onderdeel 7, van de Verordening en dat Leverancier kwalificeert als verwerker in de zin van artikel 4, onderdeel 8, van de Verordening.

De artikelen in dit model vormen één geheel met de artikelen in de Overeenkomst en de ARIV. Onderwerpen die al in de Overeenkomst of de ARIV zijn geregeld, worden daarom niet nogmaals in de Verwerkersovereenkomst geregeld. Dit model moet daarom altijd in combinatie met de Overeenkomst en de ARIV worden afgesloten.

Artikel 9 van de ARIV-2018 geeft een algemene voorziening om te borgen dat de Verwerking van Persoonsgegevens in het kader van de Overeenkomst rechtmatig is. Dit artikel is echter te beperkt om te voldoen aan alle eisen die artikel 28, derde lid, van de Verordening stelt aan een verwerkersovereenkomst.

Dit model is nadrukkelijk *niet* geschikt voor de volgende situaties:

a. Indien Koper niet kwalificeert als verwerkingsverantwoordelijke, bedoeld in artikel 4, onderdeel 7, van de Verordening, voor de Verwerking van Persoonsgegevens.
b. Indien andere algemene voorwaarden dan de ARIV van toepassing zijn verklaard op de Overeenkomst.
c. Indien de Verwerking van Persoonsgegevens niet valt onder de werkingssfeer van de Verordening, maar bijvoorbeeld onder Richtlijn (EU) 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens.
d. Indien de Persoonsgegevens worden Verwerkt in een land buiten de Europese Unie waarvoor de Europese Commissie geen adequaatheidsbesluit als bedoeld in artikel 45, derde lid, van de Verordening heeft afgegeven en geen van de in artikel 49 van de

Verordening genoemde afwijkingen op het verwerkingsverbod aan de orde is, in welk geval afspraken moet worden gemaakt die voldoen aan een van de in artikel 47, tweede of derde lid, van de Verordening genoemde situaties om te kwalificeren als passende waarborgen.

e. Indien Leverancier onderdeel is van dezelfde rechtspersoon als Leverancier, in welk geval gebruik moet worden gemaakt van de model Verwerkersafspraken Rijksdienst.

Dit model omvat 11 standaardartikelen die bij elke Verwerkersovereenkomst van toepassing zijn. De artikelen 10 en 11 van dit model kennen enkele optionele bepalingen die kunnen worden gebruikt, al naar gelang de specifieke situatie dat vereist.

Het model bevat 3 verplichte bijlagen. Deze bijlagen moeten worden ingevuld om te voldoen aan de eisen die artikel 28, derde lid, van de Verordening stelt aan een verwerkersovereenkomst. In Bijlage 1 moeten het onderwerp en doel van de Verwerking, het soort Persoonsgegevens, de categorieën Persoonsgegevens, Betrokkenen en ontvangers worden gespecificeerd. In Bijlage 2 moeten de technische en organisatorische beveiligingsmaatregelen worden gespecificeerd. In Bijlage 3 moeten de afspraken over Inbreuken in verband met Persoonsgegevens worden gespecificeerd.

II – Artikelsgewijze toelichting

Artikel 1 Begrippen

Dit artikel bepaalt allereerst dat de begripsbepalingen van artikel 1 van de ARIV-2018 ook gelden voor deze verwerkersovereenkomst. Daarnaast definieert het artikel een aantal in de Verwerkersovereenkomst gebruikte begrippen.

Betrokkene
In de Verordening wordt de betrokkene niet als zodanig gedefinieerd. In artikel 4, onderdeel 1, van de Verordening staat wel: “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”)”. In de Verwerkersovereenkomst is de definitie van artikel 1, aanhef en onder f, van de Wet bescherming persoonsgegevens gevolgd. Dit neemt niet weg dat beoogd is aan te sluiten bij de betekenis van het begrip ‘betrokkene’ in de Verordening.

Inbreuk in verband met Persoonsgegevens
Hier is de definitie van artikel 4, onderdeel 12, van de Verordening gevolgd. In de definitie is niet onderscheiden naar gelang de inbreuk al dan niet een (hoog) risico inhoudt voor de rechten en vrijheden van de Betrokkene. Dit is overigens ook slechts van belang in verband met de meldplichten van Koper bedoeld in de artikelen 33 en 34 van de Verordening.

Persoonsgegevens
Hier is de definitie van artikel 4, onderdeel 1, van de Verordening gevolgd. Aan de definitie is toegevoegd dat het enkel de gegevens betreft die Leverancier in het kader van de Overeenkomst ten behoeve van Koper verwerkt. Hiermee worden uitgesloten de persoonsgegevens die Leverancier verwerkt op basis van een andere titel dan de Overeenkomst. Bijvoorbeeld gegevensverwerkingen waarvoor Leverancier verwerkingsverantwoordelijk is.

Verwerking
Hier is de definitie van artikel 4, onderdeel 2, van de Verordening gevolgd.

Artikel 2 Voorwerp van deze Verwerkersovereenkomst

Artikel 28, derde lid, van de Verordening schrijft voor dat een verwerkersovereenkomst de Verwerking van Persoonsgegevens door een wederpartij regelt. Hierin moeten in ieder geval worden omschreven: het onderwerp en de duur van de Verwerking, de aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Betrokkenen.

In het eerste lid wordt voor de omschrijving van het onderwerp een koppeling gemaakt met de omschrijving van de dienstverlening in de Overeenkomst. In de Overeenkomst staan de diensten beschreven die Leverancier verleent.

In het tweede lid wordt verwezen naar Bijlage 1 waarin de overige aspecten moeten worden omschreven. Het gaat hier om de aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Betrokkenen. Voor het invullen van deze bijlage kan gebruik worden gemaakt van de gegevens in het departementale register van verwerkingsactiviteiten, bedoeld in artikel 30 van de Verordening.

Met soort Persoonsgegevens wordt gedoeld op de soorten: (1) bijzondere categorieën van gegevens als bedoeld in artikel 9 van de Verordening, (2) gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 van de Verordening, (3) wettelijk voorgeschreven identificatienummers en (4) overige persoonsgegevens.
Artikel 28, eerste lid, van de Verordening schrijft voor dat Koper uitsluitend een beroep mag doen op een wederpartij die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. Met het derde lid geeft Leverancier de betreffende garantie. De garantie alleen volstaat niet. De Verwerkersovereenkomst moet afspraken bevatten over de concreet door Leverancier te nemen maatregelen.

In het vierde lid wordt de garantie verbreed tot naleving van alle van toepassing zijnde wet- en regelgeving betreffende de verwerking van persoonsgegevens. Het gaat hier in eerste instantie om de Verordening en de Uitvoeringswet AVG. Daarnaast kan worden gedacht aan bijzondere wet- en regelgeving. Hiermee verbindt Leverancier zich onder meer tot het, in voorkomend geval, houden van een register van verwerkingsactiviteiten als bedoeld in artikel 30, tweede lid, van de Verordening, medewerking verlenen aan de toezichthoudende autoriteit als bedoeld in artikel 31 van de Verordening en, het aanwijzen van een functionaris voor gegevensbescherming als bedoeld in artikel 37 van de Verordening. De garantie stelt zeker dat Koper contractuele consequenties kan verbinden aan niet-nakoming van wettelijke verplichtingen door Leverancier.

Artikel 3 Inwerkingtreding en duur

Dit artikel regelt de inwerkingtreding en duur van de Verwerkersovereenkomst. Artikel 28, derde lid, aanhef, van de Verordening schrijft onder meer voor dat de duur van de Verwerking in de verwerkersovereenkomst wordt omschreven.

Het eerste lid regelt dat de Verwerkersovereenkomst tot stand komt nadat beide Partijen deze hebben ondertekend. In de praktijk zal de Verwerkersovereenkomst gelijktijdig met de Overeenkomst worden getekend en tegelijkertijd in werking treden. De Verwerkersovereenkomst dient immers voorafgaand aan de daadwerkelijke Verwerking van Persoonsgegevens gesloten te zijn.

Het tweede lid regelt dat de Verwerkersovereenkomst eindigt nadat en voorzover Leverancier alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd. In artikel 10 staat dat Leverancier na afloop van de Overeenkomst zorgdraagt voor het terugbezorgen aan Koper of het wissen van alle Persoonsgegevens. Pas nadat hieraan voldaan is, eindigt de Verwerkersovereenkomst. Het kan dus zijn dat de Verwerkersovereenkomst doorloopt (lang) nadat de Overeenkomst is geëindigd.

Overigens vloeit uit artikel 25 van de ARIV-2018 voort dat beëindiging van de Overeenkomst en de Verwerkersovereenkomst Leverancier niet ontslaat van verplichtingen daaruit die naar hun aard doorlopen. Tot deze verplichtingen behoren in ieder geval: aansprakelijkheid, geheimhouding, geschillen en toepasselijk recht.

In het derde lid is geregeld dat geen van de Partijen de Verwerkersovereenkomst tussentijds kan opzeggen. Deze bepaling is opgenomen omdat de Verwerkersovereenkomst verbonden is aan de Overeenkomst en omdat de Verordening voorschrijft dat Partijen de Verwerking van Persoonsgegevens in een overeenkomst regelen.

Artikel 4 Omvang Verwerkingsbevoegdheid Leverancier

Dit artikel bevat een aantal verplichtingen voor Leverancier die rechtstreeks voortvloeien uit (het systeem van) de Verordening.

Ingevolge artikel 29 van de Verordening Verwerkt Leverancier en eenieder die onder het gezag van Koper of Leverancier handelt en toegang heeft tot de Persoonsgegevens deze uitsluitend in opdracht van Koper, tenzij hij Unierechtelijke of lidstaatrechtelijk tot de Verwerking gehouden is. Artikel 32, vierde lid, van de Verordening bepaalt voorts dat Koper en Leverancier maatregelen treffen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van een van beiden en toegang heeft tot de Persoonsgegevens, deze slechts in opdracht van Leverancier verwerkt, tenzij hij daartoe Unierechtelijke of lidstaatsrechtelijk is gehouden. In aanvulling daarop schrijft artikel 28, derde lid, aanhef en onder a, van de Verordening voor dat een verwerkersovereenkomst in ieder geval moet bepalen dat de Persoonsgegevens uitsluitend worden verwerkt op basis van schriftelijke instructies van Koper, tenzij een op de Leverancier van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot Verwerking verplicht.

In het eerste lid is om die reden bepaald dat het Leverancier niet is toegestaan om de Persoonsgegevens in afwijking van de opdracht en/of schriftelijke instructies van Koper te Verwerken. Enige uitzondering hierop vormt de situatie dat Leverancier hiertoe gehouden is op grond van een op hem rustende wettelijke verplichting.

Indien de schriftelijke instructie van Koper naar de mening van Leverancier een inbreuk oplevert op de Verordening of een andere wettelijke bepaling inzake de bescherming van persoonsgegevens, stelt Leverancier Koper hiervan in kennis. Deze verplichting uit artikel 28, derde lid, aanhef en onder h, van de Verordening is vastgelegd in het tweede lid.

Het derde lid bepaalt dat Leverancier Koper informeert indien Koper wettelijk verplicht is om Persoonsgegevens te verstrekken, zo mogelijk voorafgaand aan de verstrekking. Artikel 28, derde lid, aanhef en onder a, van de Verordening schrijft namelijk voor dat Leverancier Koper voorafgaand aan de Verwerking in kennis stelt van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

Ingevolge artikel 4, onderdeel 7, van de Verordening is het Koper die het doel en de middelen van de Verwerking van de Persoonsgegevens vaststelt. Artikel 28, tiende lid, van de Verordening bepaalt dat als Leverancier in strijd met de Verordening en de Verwerkersovereenkomst het doel en de middelen van de Verwerking bepaalt (met andere woorden: zich niet houdt aan de eerste lid), Leverancier voor die Verwerking als Verwerkingsverantwoordelijke wordt beschouwd. De Autoriteit persoonsgegevens en Betrokkenen kunnen Leverancier hier rechtstreeks op aanspreken. In het vierde lid wordt geregeld dat Leverancier op basis van de Verwerkersovereenkomst geen zeggenschap heeft over het doel en de middelen van de Verwerking van Persoonsgegevens.

Artikel 5 Beveiliging van de Verwerking

Dit artikel gaat over de Beveiliging van de Verwerking van de Persoonsgegevens.

Artikel 32 van de Verordening verplicht de Verwerkingsverantwoordelijke en de Verwerker om passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Voorts bepaalt artikel 28, derde lid, aanhef en onder c, dat in de Verwerkersovereenkomst wordt geregeld dat Verwerker alle overeenkomstig artikel 32 vereiste maatregelen neemt. Zulks wordt in het eerste en tweede lid geregeld.

Het eerste lid verwijst naar Bijlage 2. In deze bijlage moeten de normen en maatregelen die Leverancier in het kader van de beveiliging van de Verwerking moet treffen nader worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen, de offerte of de offerteaanvraag. Bij maatregelen kan bijvoorbeeld gedacht worden aan: pseudonimiseren en versleutelen van persoonsgegevens, monitoren en loggen, screenen van personeel en fysieke maatregelen voor toegangsbeveiliging.
De maatregelen moeten, met inachtneming van de stand der techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren. Welk beschermingsniveau in een concreet geval passend is, moet worden beoordeeld op basis van een door de Koper uit te voeren risicoanalyse. Specifieke vormen van dienstverlening kunnen ook specifieke beveiligingseisen met zich brengen. Denk bijvoorbeeld aan dienstverlening binnen de cloud.

Het kan voorkomen dat niet alle Persoonsgegevens die Leverancier Verwerkt even gevoelig zijn en dat niet voor alle Verwerkte Persoonsgegevens dezelfde afspraken van toepassing zijn. In de Verwerkersovereenkomst moet in dergelijke gevallen zijn vastgelegd welke afspraken van toepassing zijn op welke Persoonsgegevens.

Ingevolge artikel 28, vierde lid, van de Verordening kan worden aangesloten bij een goedgekeurde gedragscode als bedoeld in artikel 40 van de Verordening of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 van de Verordening. Zulks is ook geregeld in artikel 32, derde lid. Denk hierbij bijvoorbeeld aan de NEN-ISO/IEC 27001 standaard inzake informatiebeveiliging.

Koper is in aanvulling op de Verordening in ieder geval gehouden aan de volgende normenkaders: het Voorschrift Informatiebeveiliging Rijksdienst 2017, het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2013 en de Baseline Informatiebeveiliging Rijksdienst 2012.

De beschrijving van de maatregelen in Bijlage 2 is niet uitputtend. Deze omschrijving in Bijlage 2 laat daarnaast reeds gestelde eisen inzake informatiebeveiliging, bijvoorbeeld in het programma van eisen, onverlet. Daarnaast kunnen op grond van het derde lid en in aanvulling op deze omschrijving aanvullende maatregelen worden verlangd door Koper. Indien gedurende de looptijd van de Verwerkersovereenkomst blijkt dat de overeengekomen maatregelen onvoldoende zijn, dient Leverancier op verzoek van Koper aanvullende maatregelen te treffen met het oog op de beveiliging van de Persoonsgegevens. Aanleiding hiervoor kan bijvoorbeeld zijn een Inbreuk op de beveiliging van de Persoonsgegevens als gevolg waarvan Persoonsgegevens zijn vernietigd, verloren gegaan of gewijzigd.

De passage ‘onverminderd artikel 2.3’ in het eerste lid, brengt tot uitdrukking dat los van de in Bijlage 2 opgenomen maatregelen, de door Leverancier getroffen maatregelen altijd passend dienen te zijn in de zin van artikel 32 van de Verordening.

Het derde lid ligt in het verlengde hiervan. Of maatregelen passend zijn, is afhankelijk van externe factoren en kan gedurende de looptijd veranderen, bijvoorbeeld door technologische ontwikkelingen of nieuwe risico’s. Partijen erkennen dit. Gevolg hiervan is dat zij gedurende de dienstverlening periodiek moeten nagaan of de getroffen maatregelen passend zijn en zo nodig aanvullende maatregelen treffen om te zorgen dat deze ‘passend’ blijven.

Het vierde lid legt vast dat Leverancier de Persoonsgegevens enkel in een land buiten de Europese Unie mag Verwerken, waaronder begrepen opslaan, indien hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Koper. Zulks behoudens afwijkende wettelijke verplichtingen die rusten op Leverancier. Ingevolge artikel 28, derde lid, aanhef en onder a, van de Verordening dient deze bepaling te worden opgenomen in een verwerkersovereenkomst.

Indien een wettelijk voorschrift Leverancier ertoe verplicht de Persoonsgegevens buiten de Europese Unie te verwerken, dient hij Koper in kennis te stellen van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Dit is geregeld in artikel 4.3.

Onder ‘buiten de Europese Unie’ wordt ook verstaan verwerking door een internationale organisatie. Ingevolge artikel 4, onderdeel 26, van de Verordening is dit een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

In de artikelen 44 tot en met 50 van de Verordening worden voorwaarden gesteld aan de doorgifte van persoonsgegevens aan derde landen en internationale organisaties. De gedachte hierachter is dat deze doorgifte niet ten koste mag gaan van het beschermingsniveau waarvan natuurlijke personen in de Europese Unie door de Verordening verzekerd zijn. Doorgifte kan alleen plaatsvinden in volledige overeenstemming met de Verordening.

Indien Partijen voornemens zijn de doorgifte van Persoonsgegevens naar een land buiten de Europese Unie te rechtvaardigen op grond van artikel 46, tweede of derde lid, van de Verordening, kan dat niet door gebruikmaking van dit model. Koper en Wederpartij dienen specifieke afspraken te maken om passende waarborgen te bieden gelet op de bijzondere risico’s ten gevolge van Verwerkingen in een land buiten de Europese Unie.

Het vijfde lid verplicht Leverancier om Koper zonder onredelijke vertraging te informeren over onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op de beveiligingsmaatregelen. Het is vervolgens aan Koper om te beoordelen of zulks kwalificeert als een meldenswaardige Inbreuk in verband met Persoonsgegevens als bedoeld in de artikelen 33 en 34 van de Verordening.

Koper moet inzicht hebben in alle onrechtmatige verwerkingen van Persoonsgegevens of inbreuken op de beveiligingsmaatregelen. Ingevolge artikel 33, vijfde lid, van de Verordening moet Koper namelijk alle Inbreuken in verband met Persoonsgegevens, met inbegrip van de feiten over de Inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen, documenteren, teneinde de toezichthoudende autoriteit in staat te stellen de naleving van de artikelen 33 en 34 te controleren.

Tot slot regelt het zesde lid dat Leverancier Koper bijstand verleent bij het doen nakomen van de verplichtingen genoemd in de artikelen 32 tot en met 36 van de Verordening. Ingevolge artikel 38, derde lid, aanhef en onder f, van de Verordening dient zulks te zijn opgenomen in de Verwerkersovereenkomst. In deze artikelen gaat het om de verplichtingen tot: het treffen van beveiligingsmaatregelen (artikel 32), het melden van een Inbreuk in verband met Persoonsgegevens aan de toezichthoudende autoriteit en de Betrokkene (artikelen 33 en 34), het uitvoeren van een gegevensbeschermingseffectbeoordeling (artikel 35) en de voorafgaande raadpleging van de toezichthoudende autoriteit (artikel 36).

Artikel 6 Geheimhouding door Personeel van Leverancier

Artikel 28, derde lid, aanhef en onder b, van de Verordening schrijft voor dat in de Verwerkersovereenkomst wordt bepaald dat de Leverancier waarborgt dat de tot het Verwerken van de Persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

Het eerste lid bepaalt dat de Persoonsgegevens een vertrouwelijk karakter hebben zoals bedoeld in artikel 8 van de ARIV-2018. In artikel 8, eerste lid, van de ARIV-2018 is reeds geregeld dat Leverancier hetgeen hem bij de uitvoering van de Overeenkomst ter kennis komt, en waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden, op geen enkele wijze verder bekend maakt, behalve voor zover enig wettelijk voorschrift of uitspraak van de rechter hem tot bekendmaking daarvan verplicht. In aanvulling daarop regelt het tweede lid van artikel 8 van de ARIV-2018 dat Leverancier zijn personeel verplicht tot het nakomen van deze geheimhoudingsverplichting. Het vierde lid biedt de mogelijkheid om bij de Overeenkomst een boete te stellen op het schenden van de geheimhoudingsverplichting.

Het tweede lid legt de verplichting voor Leverancier vast om op verzoek van Koper aan te tonen dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen. Dit kan bijvoorbeeld aan de hand van het overleggen van een door het Personeel ondertekende geheimhoudingsverklaring.

Artikel 7 Subverwerkers

Ingevolge artikel 28, tweede lid, van de Verordening zet Leverancier geen andere verwerker in zonder voorafgaande specifieke of algemene schriftelijke toestemming van Koper. Ingevolge artikel 28, derde lid, aanhef en onder d, van de Verordening moet dit schriftelijk worden overeengekomen.

Ingevolge artikel 28, vierde lid, van de Verordening moet Leverancier de door hem ingeschakelde verwerkers dezelfde verplichtingen inzake de bescherming van Persoonsgegevens opleggen als die welke tussen hem en Koper zijn overeengekomen. Daarnaast bepaalt het artikel dat wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, Leverancier ten aanzien van Koper volledig aansprakelijk blijft voor het nakomen van de verplichtingen van die andere verwerkers. Artikel 28, derde lid, aanhef en onder d, van de Verordening schrijft voor dat dit moet worden opgenomen in de overeenkomst.

Artikel 8 Bijstand vanwege rechten van Betrokkene

Artikel 28, derde lid, aanhef en onder e, van de Verordening bepaalt dat Leverancier Koper bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgestelde rechten van betrokkene te beantwoorden. Dit is vastgelegd in artikel 8.

Het gaat hier om de rechten van Betrokkene genoemd in artikel 12 tot en met artikel 22 van de Verordening. Dit zijn het recht op informatie en toegang tot de Persoonsgegevens, rectificatie, gegevenswissing, beperking en overdraagbaarheid van Persoonsgegevens, alsmede het recht van bezwaar.

Artikel 9 Inbreuk in verband met Persoonsgegevens

In aanvulling op de verplichting genoemd in artikel 5.4 regelt het eerste lid de wijze waarop Leverancier Koper dient te informeren over Inbreuken in verband met Persoonsgegevens (datalekken). In Bijlage 3 moet worden vastgelegd hoe Leverancier Koper informeert en welke informatie Leverancier Koper ten minste moet verstrekken.

Op basis van de informatie moet Koper kunnen bepalen of sprake is van een meldingswaardige Inbreuk in verband met Persoonsgegevens als bedoeld in de artikelen 33 en 34 van de Verordening. Tevens moet Koper hierdoor kunnen voldoen aan zijn verplichting om alle inbreuken te registreren (artikel 33, vierde lid, van de Verordening). Artikel 9 ligt daarmee ook in het verlengde van artikel 28, derde lid, aanhef en onder f, van de Verordening.

In het tweede lid is opgenomen dat Leverancier Koper ook na een melding op grond van het eerste lid moet informeren over ontwikkelingen betreffende een Inbreuk in verband met Persoonsgegevens, opdat Koper kan voldoen aan zijn verplichtingen onder meer genoemd in de artikelen 33 en 34 van de Verordening.

Het derde lid legt vast dat Partijen hun eigen kosten dragen die gemoeid zijn met de melding van de Inbreuk in verband met Persoonsgegevens aan de Autoriteit persoonsgegevens.

Artikel 10 Teruggave Persoonsgegevens

Dit artikel hangt samen met artikel 3 inzake de duur van de Verwerkersovereenkomst. Ingevolge het tweede lid eindigt deze Verwerkersovereenkomst pas nadat en voor zover Leverancier alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd. Het kan dus zijn dat deze Verwerkersovereenkomst van kracht blijft (lang) nadat de Overeenkomst is beëindigd.

Ingevolge artikel 28, derde lid, aanhef en onder g, van de Verordening dient in de Verwerkersovereenkomst geregeld te worden dat Leverancier na afloop van de Verwerkingen, naargelang de keuze van Koper, alle Persoonsgegevens wist of deze aan Koper terugbezorgt, en bestaande kopieën verwijdert, tenzij Leverancier wettelijk verplicht is de Persoonsgegevens op te slaan. Dit is geregeld in het eerste lid.

Het tweede lid is een optionele bepaling. Door opname van deze bepaling kan geregeld worden binnen welke termijn na afloop van de Overeenkomst Leverancier de Persoonsgegevens dient te wissen of terug te bezorgen. Voorts bepaalt het artikel dat Leverancier aan Koper een boete verschuldigd is per dag dat hij in gebreke is. De hoogte van de boete en het maximale bedragen dienen te worden ingevuld. De ingevulde bedragen dienen proportioneel te zijn.

Het derde lid is eveneens een optionele bepaling. In dit model zijn twee alternatieve mogelijkheden opgenomen. Deze alternatieven zien op het geval de Persoonsgegevens moeten worden terugbezorgd aan Koper. In het eerste alternatief wordt geregeld dat de vorm waarin de Persoonsgegevens moeten worden terugbezorgd, te zijner tijd door Koper wordt aangegeven. In het tweede alternatief wordt de wijze van terugbezorging opgenomen in de Verwerkersovereenkomst.

Artikel 11 Informatieverplichting en audit

Koper moet erop (kunnen) toezien dat Leverancier, en eventuele andere verwerkers, zich aan de afspraken uit de Verwerkersovereenkomst houden. Ingevolge artikel 28, eerste lid, van de Verordening kan Koper uitsluitend een beroep doen op Leverancier, indien deze afdoende garanties biedt met betrekking tot het toepassen van passende maatregelen opdat de Verwerking voldoet aan de vereisten van de Verordening en de bescherming van de rechten van Betrokkene is gewaarborgd.

Op grond van artikel 28, derde lid, aanhef en onder h, van de Verordening moet in de Verwerkersovereenkomst worden opgenomen dat Leverancier Koper alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door Koper of een door Koper gemachtigde controleur mogelijk maakt en eraan bijdraagt. Zulks is vastgelegd in het eerste en tweede lid.

Het derde lid is een facultatieve bepaling met twee opties. De eerste optie gaat uit van de situatie dat Koper een audit laat uitvoeren door een onafhankelijke partij. Bepaald moet worden hoe vaak Koper hiertoe overgaat. De tweede optie gaat uit van de situatie dat Leverancier een onafhankelijke externe deskundige een audit laat uitvoeren. Bepaald moet worden hoe vaak Leverancier hiertoe opdracht geeft en uiterlijk voor welke datum.

Indien uit de audit blijkt dat de getroffen beveiligingsmaatregelen onvoldoende zijn, kan Koper op grond van artikel 5.2 Leverancier verlangen aanvullende maatregelen te treffen, opdat een passend beveiligingsniveau geborgd is.

III - Transponeringstabel

AVG	*Model*	*ARIV*
28.1	2.3, 11	9.1
28.2	7	
28.3	2.1, 2.3, 3, Bijlage 1	9.2
28.3.a	4.1, 4.3, 5.3	
28.3.b	6.1	8
28.3.c	5.1, Bijlage 2	
28.3.d	7	
28.3.e	8	
28.3.f	5.2, 5.4, 5.5, 9.1, Bijlage 2 en 3	
28.3.g	3.2, 10.1	
28.3.h	4.2, 11.1	
28.4	7	
28.10	4.4	

Colofon

Deze toelichting is opgesteld onder verantwoordelijkheid van de Commissie Bedrijfsjuridisch Advies (CBA) van de Rijksoverheid.

Nadere inlichtingen kunnen ingewonnen worden bij het secretariaat van de CBA (cba@minbzk.nl).

Uitgegeven mei 2018