INFORMATIE
BEVEILIGINGS
DIENST

FACTSHEET VERWERKERSOVEREENKOMSTEN

Bij de verwerking van persoonsgegevens maken gemeenten in sommige gevallen gebruik van diensten van derde partijen. De uitvoering van verwerkingen van persoonsgegevens door een derde partij moet geregeld worden in een overeenkomst, de verwerkersovereenkomst. Deze overeenkomst moet schriftelijk of in elektronische vorm zijn vastgelegd. U leest in deze factsheet alles over de wettelijke verplichtingen ten aanzien van de afspraken. Deze factsheet biedt houvast bij het bepalen of een verwerkersovereenkomst verplicht is en wat er vervolgens in de overeenkomst moet zijn opgenomen. Ook in gevallen waarin een verwerkersovereenkomst niet wettelijk verplicht is, loont het de moeite om afspraken te maken met leveranciers en derde partijen over de omgang met persoonsgegevens en de verdeling van wettelijke taken.

Iedereen heeft recht op bescherming van zijn of haar persoonsgegevens (art. 10 lid 1 van de grondwet, art. 8 Handvest van de grondrechten van de EU, en art. 16 lid 1 Verdrag betreffende de werking van de Europese Unie (VWEU)). Deze bescherming is vastgelegd in de Richtlijn bescherming persoonsgegevens (95/46/EG). Deze richtlijn is in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). Per 25 mei 2018 is echter de algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum nog maar één privacywet geldt in de hele Europese Unie (EU).[1] In het licht van de toenemende digitalisering en de juridische wijzigingen zijn gemeenten actief aan de slag om in hun dienstverlening de privacy van inwoners te waarborgen. Dit geldt intern maar ook in de samenwerking met toeleveranciers en dienstverleners.

1 Kijk voor meer informatie op https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming

GEMEENTEN EN LEVERANCIER MOETEN SAMEN AFSPRAKEN MAKEN OVER TAKEN EN VERANTWOORDELIJKHEDEN IN HET KADER VAN VEILIGE VERWERKING VAN PERSOONSGEGEVENS.

VERANTWOORDELIJKE EN VERWERKER

Gemeenten hebben steeds vaker (een deel van) hun persoonsgegevens buiten de deur staan bij een derde partij of maken gebruik van derden die in opdracht van deze gemeenten persoonsgegevens verwerkt. Deze derde partijen kwalificeren veelal als 'bewerker' (Wbp) en / of 'verwerker' (AVG)[1]. Met de komst van de AVG zijn de begrippen verantwoordelijke (controller) en bewerker (processor) gewijzigd in verwerkingsverantwoordelijke en verwerker.

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

1 De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

WETTELIJKE VERPLICHTINGEN

Uit de wet volgt dat elke handeling (verwerking of bewerking) met betrekking tot persoonsgegevens die tot een natuurlijk persoon[1] herleidbaar zijn (persoonsgegevens), aan bepaalde eisen is gebonden.

BEWERKERS- / VERWERKERSOVEREENKOMST

De uitvoering van verwerkingen door een verwerker dient geregeld te worden in een overeenkomst, de verwerkersovereenkomst, of in een wettelijke regeling tussen een verwerkingsverantwoordelijke en een verwerker. De overeenkomst moet schriftelijk of in elektronische vorm zijn vastgelegd.[2] Bindende afspraken tussen de verwerkingsverantwoordelijke en verwerker kunnen ook blijken uit andere rechtshandelingen, mits voldaan wordt aan de vereisten. Volgens de AVG kunnen de verwerkingsverantwoordelijke en verwerker in plaats van een individuele verwerkersovereenkomst ook 'standaardcontractbepalingen' gebruiken.[3] De verwerkersovereenkomst geeft de keten in het proces van verwerking tussen de verwerkingsverantwoordelijke, verwerkers en subverwerkers weer en geeft inzicht in de verdeling van verantwoordelijkheden en aansprakelijkheden. De kern hierbij is dat de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking.[4]
Bij het inschakelen van verwerkers door de verwerkingsverantwoordelijke is het belangrijkste uitgangspunt dat deze verwerkers voldoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten voldoen en de bescherming van de rechten van de betrokkene is gewaarborgd.[5]

REGISTER VAN DE VERWERKINGSACTIVITEITEN

Verwerkingsverantwoordelijke en verwerkers moeten een schriftelijke (of elektronische) administratie (register) bijhouden, waarin alle activiteiten worden omschreven waarbij persoonsgegevens worden verwerkt, van alle verwerkingen, inclusief contactgegevens, het doel, de juridische grondslag, categorieën van betrokkenen, de persoonsgegevens, de ontvangers van de persoonsgegevens, een beschrijving van de beveiligingsmaatregelen en de beoogde bewaartermijnen, om de accountability[6] te vergroten.[7] Op verzoek van de toezichthouder, de Autoriteit Persoonsgegevens (AP)[8], dient de administratie aan de toezichthouder (AP) overhandigd te worden ter controle.[9] Deze administratie is verplicht voor alle gemeenten.[10]

MELDEN DATALEKKEN

Naast de meldplicht datalekken in de Wbp[11] kent ook de AVG[12] een meldplicht datalekken, de term in de AVG is 'een inbreuk in verband met persoonsgegevens' in plaats van datalek. Op het moment dat er per ongeluk, of opzettelijk, data verloren gaan, of op straat terecht gekomen zijn, moet dit binnen 72 uur aan de toezichthouder (AP) gemeld worden.

ADMINISTRATIEPLICHT

Behalve een meldplicht datalekken bevat de Wbp ook een administratieplicht.[13] De verwerkingsverantwoordelijke moet een overzicht bijhouden van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en persoonsgegevens omtrent de aard van de inbreuk, alsmede de tekst van de kennisgeving aan de betrokkene. De AVG kent een veel grotere administratieplicht dan nu onder de Wbp het geval is. De verwerkingsverantwoordelijke administreert 'alle inbreuken', dus ook de niet meldingsplichtige.[14] Onder de Wbp en de AVG is het niet verplicht om afspraken te maken over het bijhouden van een administratie over meldingsplichtige datalekken door de verwerker en doorgeven van de administratieplicht van de verwerker aan de verwerkingsverantwoordelijke. Het advies is dat de verwerkingsverantwoordelijke hierover in de verwerkersovereenkomst wel afspraken maakt en te regelen dat de verwerker de administratie bijhoudt. De toezichthouder (AP) kan immers vragen om inzage in die (wettelijk verplichte) administratie. Als die administratie er niet blijkt te zijn, kan de toezichthouder (AP) handhavend optreden en zelfs boetes opleggen.

1 https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens
2 Artikel 28 lid 9 AVG
3 Artikel 28 lid 7 en 8 AVG
4 Artikel 29 AVG en het overeenkomstige artikel 12 lid 1 Wbp
5 Artikel 28 AVG en het overeenkomstige artikel 14 Wbp
6 De verwerkingsverantwoordelijke moet verantwoording/rekenschap afleggen over de bescherming van persoonsgegevens. aangezien het zijn verantwoordelijkheid is.
7 Artikel 30 AVG lid 1, 2 en 3
8 https://autoriteitpersoonsgegevens.nl
9 Artikel 30 lid 4 AVG
10 Artikel 30 lid 5 AVG
11 Artikel 34a Wbp
12 Artikel 33 en 34 AVG
13 Artikel 34a lid 8 Wbp
14 Artikel 33 lid 5 AVG

GIBIT & MODEL VERWERKERSOVEREENKOMST IBD

De Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) gaat over de verhouding tussen partijen en de in dat kader (al dan niet aanvullend) te maken afspraken. Leverancier neemt de rol van verwerker in.[1] De GIBIT heeft in dit kader te gelden als (basis)verwerkersovereenkomst.[2] Daar waar de afspraken uit de GIBIT niet volstaan, kan een aanvullende of afwijkende verwerkersovereenkomst worden gesloten.[3] Hiervoor is een model verwerkersovereenkomst beschikbaar gesteld.[4] Naast de GIBIT model verwerkersovereenkomst wordt er ook een model verwerkersovereenkomst vanuit KING/IBD beschikbaar gesteld voor de overeenkomsten die afgesloten worden en niet gerelateerd zijn aan IT.[5]

1 Artikel 24 GIBIT
2 Artikel 24.2 GIBIT
3 Artikel 24.3 GIBIT
4 Zie hiervoor de website van GIBIT (http://www.gibit.nl)
5 Zie hiervoor www.ibdgemeenten.nl

VERPLICHTE AFSPRAKEN

In bijlage 1 wordt een overzicht op hoofdlijnen gegeven van de inhoud van een verwerkersovereenkomst. In een verwerkersovereenkomst moet het volgende worden beschreven ten aanzien van de verwerking.[1]

- het onderwerp
- de duur
- de aard
- het doel
- de omgang met de data bij beëindiging
- het soort persoonsgegevens
- de categorieën van betrokkenen
- de rechten en verplichtingen van de verwerkingsverantwoordelijke
- de mogelijkheid voor de verwerkingsverantwoordelijke om te kunnen controleren of de verwerker zich houdt aan de gemaakte afspraken, bijvoorbeeld door het uitvoeren van audits.

In bijlage 2 wordt een overzicht gegeven van wanneer wel en wanneer wettelijk gezien geen verwerkersovereenkomst opgesteld dient te worden, het blijft evenwel mogelijk en zelfs aan te raden om afspraken te maken.

1 Artikel 28 lid 3 AVG

NIEUW IN DE AVG

VOORSCHRIFTEN OVER INVULLING VERWERKERSOVEREENKOMSTEN

De AVG bevat (uitgebreide) voorschriften over de verhouding tussen de verwerkingsverantwoordelijke en de verwerker, het inschakelen van een verwerker en wordt gedetailleerd voorgeschreven waaraan een verwerkersovereenkomst moet voldoen.[1] De dwingend voorgeschreven invulling van een verwerkersovereenkomst is nieuw ten opzichte van de Wbp.

SUBVERWERKERS ALLEEN MET TOESTEMMING

Een nieuwe vereiste ten opzichte van de Wbp is dat verwerkers geen subverwerker in dienst mogen nemen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke.[2]

GROTERE ADMINISTRATIEPLICHT

De verwerkingsverantwoordelijke moet een overzicht bijhouden van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. De AVG kent een veel grotere administratieplicht dan nu onder de Wbp het geval is. De verwerkingsverantwoordelijke administreert 'alle inbreuken', dus ook de niet meldingsplichtige.[3]

MELDPLICHT DATALEKKEN IN DE AVG

Het verschil met de huidige meldplicht datalekken (Wbp) is dat onder de AVG geen meldplicht geldt als de verwerkingsverantwoordelijke kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van betrokkenen (de personen waar de persoonsgegevens betrekking op hebben) met zich brengt. Als de inbreuk in verband met persoonsgegevens waarschijnlijk hoge risico's voor de betrokkenen met zich kan brengen, dan moeten zij ook van de inbreuk in verband met persoonsgegevens op de hoogte worden gesteld. Het volgende verschil met de huidige meldplicht datalekken, is dat er enkel een melding bij de AP gedaan hoeft te worden van een inbreuk in verband met persoonsgegevens als de inbreuk daadwerkelijk heeft plaatsgevonden. Er hoeft dus niet gemeld te worden als het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Onze huidige meldplicht datalekken (Wbp) noemt een incident al een datalek wanneer de onrechtmatige verwerking van persoonsgegevens niet uitgesloten (mogelijk datalek) kan worden. Daarnaast kent de AVG aan de verwerker een verplichting toe om de inbreuk aan de verwerkingsverantwoordelijke te melden. In de verwerkersovereenkomst dient te worden bepaald dat de verwerker rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van onder andere de melding inbreuk in verband met persoonsgegevens.

1 Artikel 33 en 34 AVG
2 Artikel 34a lid 8 Wbp
3 Artikel 33 lid 5 AVG

IBD ADVIEZEN & UITGANGSPUNTEN AFSPRAKEN LEVERANCIERS EN GEMEENTEN

De IBD adviseert de gemeente te beginnen met het maken van een overzicht van alle leveranciers die in opdracht van de gemeente diensten verlenen die betrekking hebben op de verwerking van persoonsgegevens. Vervolgens kan worden nagegaan of met alle leveranciers afspraken zijn gemaakt en of deze aangepast moeten worden naar de regels van de AVG.[1] Onderstaand treft u de twee belangrijkste uitgangspunten als leverancier en gemeenten met elkaar in overleg gaan over de verwerkersovereenkomst:

- Gemeenten en leverancier moeten samen afspraken maken over taken en verantwoordelijkheden in het kader van veilige verwerking van persoonsgegevens. De manier waarop dit geregeld wordt is niet in beton gegoten maar de gekozen constructie moet altijd voldoen aan de wet.
- De gemeente moet met de leverancier in overleg over de invulling van de afspraken rondom de veilige verwerking van persoonsgegevens en de partijen leggen vervolgens deze afspraken schriftelijk vast in een verwerkersovereenkomst.

De IBD adviseert leveranciers en gemeenten minimaal afspraken te maken over de volgende wettelijke verplichtingen:

- De waarborgen die de leverancier biedt ten aanzien van technische en organisatorische maatregelen en de manier waarop de gemeente dit kan controleren.
- De wijze waarop de gemeente wordt geïnformeerd bij een beveiligingsincident en te regelen dat de leverancier de administratie bijhoudt.
- De aansprakelijkheid bij schade doordat in strijd met de wet wordt gehandeld.
- De mate waarin de dienstverlening voldoet aan de wettelijke eisen.

Bij de afspraken is het goed om te beseffen dat zowel de leverancier als de gemeente een belang heeft bij redelijke eisen. De gemeente moet zijn verantwoordelijkheid kunnen nemen bij de uitbesteding van verwerkingen van persoonsgegevens. Tegelijkertijd moet de leverancier een gezonde bedrijfsvoering kunnen uitoefenen. De leverancier is gebaat bij tevreden klanten en de klant is gebaat bij een leverancier die op de lange termijn de dienstverlening kan verzorgen.

1 Artikel 28 lid 3 AVG

DEZE FACTSHEET IS OPGESTELD IN SAMENWERKING MET DE VERENIGING NEDERLANDSE GEMEENTEN.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.

BIJLAGE 1: INHOUD VERWERKERSOVEREENKOMST

De wet bepaalt niet precies wat er in de verwerkersovereenkomsten moet staan. In de praktijk komen in de verschillende verwerkersovereenkomsten globaal genomen wel dezelfde basisonderwerpen voor, namelijk:

- onderwerp en doel van de overeenkomst;
- te verwerken persoonsgegevens;
- beveiligingsmaatregelen;
- rapportages over de beveiliging;
- beveiligingsincidenten en datalekken;
- doorgifte van persoonsgegevens buiten Nederland/ de EU;
- locatie van de data;
- verstrekking van persoonsgegevens aan derden;
- geheimhouding;
- verzoeken van betrokkenen;
- aansprakelijkheid;
- controle-/auditmogelijkheden;
- wijzigingen of beëindiging van de verwerkersovereenkomst
- overdracht en vernietiging van persoonsgegevens na afloop van de overeenkomst;
- bewaar-, back-up- en vernietigingsprocessen.

Bij de verwerkersovereenkomsten moet ook rekening worden gehouden met de meldplicht datalekken. De verwerkingsverantwoordelijke moet er namelijk sinds 1 januari 2016 voor zorgen dat de verwerker maatregelen treft om aan de meldplicht datalekken te kunnen voldoen en toezien op de naleving hiervan.[1] De verwerkersovereenkomsten zijn in de AVG uitgebreider geregeld dan in de Wbp. Bijvoorbeeld dat de verwerker geen andere subverwerker in dienst mag nemen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke.[2] In veel verwerkersovereenkomsten komt dit nu ook al terug in de vorm van een verplichting tot het verstrekken van informatie over subverwerkers. Overigens is in de AVG uitgewerkt welke onderwerpen er verplicht in een verwerkersovereenkomst moeten worden opgenomen.[3] Deze onderwerpen komen grotendeels overeen met de bovengenoemde basisonderwerpen van de Wbp, maar bevatten ook een aantal geëxpliciteerde plichten voor de verwerker, zoals de plicht om:

- de persoonsgegevens uitsluitend te verwerken op basis van de schriftelijke instructies van de verwerkingsverantwoordelijke;[4]
- de vertrouwelijkheid in acht te nemen;[5]
- passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen;[6]
- bijstand te verlenen als de betrokkene een van zijn rechten uitoefent;[7]
- na afloop van de verwerkingsdiensten, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert;[8]
- medewerking te verlenen bij audits;[9]
- de verwerkingsverantwoordelijke zonder onredelijke vertraging te informeren zodra de verwerker kennis heeft genomen van een inbreuk in verband met persoonsgegevens;[10]
- met een eventuele subverwerker dezelfde afspraken te maken als die gelden tussen de verwerkingsverantwoordelijke en de verwerker.[11]

Het merendeel van deze onderwerpen komen nu ook al terug in verwerkersovereenkomsten, maar met de AVG komt hier echter een wettelijke verankering voor.

OMSCHRIJVING VAN DE PERSOONSGEGEVENS/ ONDERWERP VAN DE OVEREENKOMST

In het eerste gedeelte van de verwerkersovereenkomst dient een omschrijving van de inhoud, de duur van de verwerking, het doel van de verwerking, soorten persoonsgegevens en categorieën van betrokkenen te worden opgenomen. Tevens omschrijft dit gedeelte ook de rechten en plichten van de verwerkingsverantwoordelijke ten aanzien van de verwerker.

DIENSTVERLENING

De verwerkersovereenkomst moet beschrijven welke diensten de verwerker verleent met betrekking tot de persoonsgegevens (voor de verwerkingsverantwoordelijke). De verwerking moet in overeenstemming zijn met instructies van de verwerkingsverantwoordelijke. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verwerkingsverantwoordelijke. Er zullen afspraken gemaakt moeten worden omtrent de geheimhouding van de persoonsgegevens en over de geheimhouding van de personen die ten behoeve van de diensten werken met deze persoonsgegevens.

BETROUWBAARHEIDSEISEN

Persoonsgegevens kunnen onder verschillende categorieën worden onderverdeeld.[12] Voor ieder van de verschillende categorieën dienen afspraken vastgelegd te worden in de verwerkersovereenkomst.

BEVEILIGING EN CONTINUÏTEIT

In de verwerkersovereenkomst moeten afspraken worden gemaakt betreffende de (technische en organisatorische) beveiliging van de persoonsgegevens om zorg te dragen voor de vertrouwelijkheid, integriteit en beschikbaarheid van de persoonsgegevens.[13] De verwerkingsverantwoordelijke draagt zorg dat de verwerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen tegen verlies et cetera. De afspraken mogen niet algemeen zijn en moeten gedetailleerd worden vastgelegd.

TRANSPARANTIE OVER DE BEVEILIGING

De verwerker en de verwerkingsverantwoordelijke moeten ook afspraken maken over de rapportages over de beveiliging. In de verwerkersovereenkomst dienen de inhoud en de frequentie van de rapportages te worden vastgelegd. Ook moet de verwerkingsverantwoordelijke het recht hebben om de gehanteerde beveiligingseisen door de verwerker door een deskundige te laten inspecteren.

1 Artikel 14 lid 1 en lid 3c Wbp
2 Artikel 28 lid 2 AVG
3 Artikel 28 lid 3 AVG
4 Artikel 28 lid 3a AVG
5 Artikel 28 lid 3b AVG
6 Artikel 28 lid 3c en Artikel 32 AVG
7 Artikel 28 lid 3e AVG
8 Artikel 28 lid 3g AVG
9 Artikel 28 lid 3h AVG
10 Artikel 28 lid 3f en Artikel 33 lid 2 AVG
11 Artikel 28 lid 4 AVG
12 Artikel 16 Wbp en Artikel 9 lid 1 AVG.
13 Artikel 14 lid 1 Wbp en Artikel 28 lid 1 AVG

TRANSPARANTIE OVER BEVEILIGINGSINCIDENTEN EN DATALEKKEN

Transparantie gaat over de inhoud van de rapportages van beveiligingsincidenten en de snelheid waarmee moet worden gerapporteerd. Als zich een beveiligingsincident heeft voorgedaan is het belangrijk dat er wordt gerapporteerd aan de verwerkingsverantwoordelijke en – eventueel – de betrokkenen. In de afspraken moet worden opgenomen dat en op welke wijze de verwerker beveiligingsincidenten en datalekken die (mogelijk) gevolgen hebben voor betrokkenen meteen rapporteert aan de verwerkingsverantwoordelijke. Tevens moet worden vastgelegd dat de verwerker bij een beveiligingsincident waar nodig meewerkt aan het adequaat informeren van betrokkenen.

VERWERKING VAN DE PERSOONSGEGEVENS BUITEN NEDERLAND/EU

Een ander belangrijk onderdeel van de verwerkersovereenkomst gaat over afspraken over welke persoonsgegevens in welke landen worden verwerkt (met name van belang: opgeslagen) en onder welke voorwaarden. Let op: wanneer persoonsgegevens buiten de EU[1] worden verwerkt zijn extra waarborgen voor de verwerking van de persoonsgegevens vereist. Het doorgeven van persoonsgegevens buiten de EU mag alleen wanneer dit land of de organisatie voldoende bescherming biedt.

LOCATIE VAN DE DATA

De verwerkingsverantwoordelijke moet weten in welke landen zijn data worden opgeslagen. Dit is mede van belang met het oog op de verplichtingen die gelden bij doorgifte van persoonsgegevens naar het buitenland. Het is noodzakelijk om hierover afspraken te maken en deze vast te leggen in de verwerkingsovereenkomst.

VERWERKING DOOR SUBVERWERKERS

In de verwerkersovereenkomst wordt vastgelegd of, en onder welke voorwaarden, de verwerker subverwerkers mag inschakelen. Er moet overeenstemming bereikt worden over het al dan niet toestaan van verwerking door subverwerkers. Wanneer een verwerker de verwerking van (een deel van de) persoonsgegevens uitbesteedt aan een derde partij of onderaannemer, dan wordt deze partij een subverwerker genoemd. Een nieuwe vereiste ten opzichte van de Wbp is dat verwerkers geen subverwerker in dienst mogen nemen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke.[2]

GEHEIMHOUDING

Afspraken omtrent de geheimhouding van de persoonsgegevens en over de geheimhouding van de personen die ten behoeve van de diensten uitvoering geven aan de gegevensverwerking.[3, 4] Hier dient aan de verwerker een geheimhoudingsplicht opgelegd te worden, eventueel gecombineerd met een boetebeding. Overigens is het opzettelijke niet naleven van deze geheimhoudingsplicht strafbaar gesteld in het Wetboek van Strafrecht.

VERZOEKEN VAN BETROKKENEN

In de verwerkersovereenkomst dienen afspraken te worden gemaakt over de wijze waarop de verwerker zijn medewerking dient te verlenen aan verzoeken van betrokkenen om inzage[5], verbetering, aanvulling, verwijdering en afscherming[6] van zijn/haar persoonsgegevens waar de verwerker toegang tot heeft.

AANSPRAKELIJKHEID

De wet bepaalt dat de verwerkingsverantwoordelijke kan worden aangesproken als iemand schade lijdt doordat de wet niet wordt nageleefd.[7] Dit geldt zelfs als de schade het gevolg is van nalatigheid van de verwerker, die in dat geval ook zelfstandig aansprakelijk is. De aansprakelijkheidsverdeling van verwerkingsverantwoordelijke en verwerker voor de schade voortvloeiende uit het niet nakomen van de afspraken die zijn vastgelegd in de verwerkersovereenkomst moet worden geregeld.

CONTROLE EN AUDITS

Er dienen afspraken te worden gemaakt over de mogelijkheid voor de verwerkingsverantwoordelijke om te kunnen controleren of de verwerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verwerkingsverantwoordelijke of door een onafhankelijke derde. In de verwerkersovereenkomst moeten de mogelijkheden over het uitvoeren van audits worden vastgelegd.
Verder dient in de verwerkersovereenkomst aandacht te worden besteed aan de rangorde van overeenkomsten tussen verwerkingsverantwoordelijke en verwerker en het toepasselijk recht.

WIJZIGINGEN OF BEËINDIGING VAN DE VERWERKERSOVEREENKOMST

In de verwerkersovereenkomst moeten afspraken worden opgenomen over het wijzigen of beëindiging van de verwerkersovereenkomst. Ook een noodplan voor het geval één van de partijen de verwerkersovereenkomst wil beëindigen dient opgenomen te worden. Verder wordt hierin vastgelegd hoe de verwerkingsverantwoordelijke, na beëindiging van de dienstverlening door verwerker, de verwerkte persoonsgegevens weer ter beschikking krijgt. Ook moet er worden vastgelegd hoe wordt gewaarborgd dat de verwerker na het beëindigen van de verwerkersovereenkomst niet meer over de persoonsgegevens kan beschikken.

BEWAARTERMIJNEN, BACK-UP EN VERNIETIGING

Het is nodig afspraken op te nemen in de verwerkersovereenkomst omtrent de bewaartermijnen, reservekopieën en vernietiging van de persoonsgegevens (bij beëindiging van de verwerkersovereenkomst).[8]

Tot slot kan de AP volgens de AVG modelovereenkomsten en/of modelbepalingen voor een verwerkersovereenkomst opstellen.[9]

1 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu
2 Artikel 28 lid 2 AVG
3 Artikel 12 lid 2 Wbp en Artikel 90 AVG
4 https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-2-voorwaarden-voor-de-rechtmatigheid-van-de-verwerking-v-22
5 Artikel 35 Wbp en Artikel 15 AVG
6 Artikel 36 Wbp en voor recht op rectificatie Artikel 16 AVG en recht op gegevenswissing/vergetelheid artikel 17 AVG
7 Artikel 49 Wbp en Artikel 82 AVG
8 Artikel 28 lid 3g AVG
9 Artikel 28 lid 7 en 8 AVG

BIJLAGE 2: VOORBEELDSITUATIES WANNEER WEL EN WANNEER GEEN VERWERKERSOVEREENKOMST[1]

Verwerken is een ruim begrip; als een derde partij bij de door de gemeente verzamelde persoonsgegevens kan, wordt deze voor de wet al gezien als verwerker. Let hierbij op dat een derde partij ook zelf verwerkingsverantwoordelijke kan zijn.

Wanneer de gemeente persoonsgegevens laat verwerken door een derde partij (leverancier) in opdracht van de gemeente, is de derde partij (leverancier) een verwerker. Het juridisch criterium van 'opdracht' is of de gemeente doel en middelen vaststelt van het verwerken. Als de gemeente besluit bepaalde gegevensverwerkingen uit te besteden, dienen de nodige afspraken tussen beide partijen te worden vastgelegd in de vorm van een verwerkersovereenkomst. Ook is het belangrijk te weten dat de persoonsgegevens enkel in opdracht, en volgens de aanwijzingen die zijn opgenomen in een verwerkersovereenkomst, van de verwerkingsverantwoordelijke mogen worden verwerkt. De verwerker mag de persoonsgegevens waar de verwerker over komt te beschikken dus niet op eigen gezag voor een heel ander doel gaan verwerken. Het is overigens de verwerkingsverantwoordelijke die na dient te gaan of dit alles ook daadwerkelijk gebeurt. De verwerkingsverantwoordelijke blijft echter verantwoordelijke en zal dus moeten letten op wat er precies in deze verwerkersovereenkomst staat en of dat voldoende is.

Wanneer de gemeente persoonsgegevens laat verwerken door een derde partij, dient de gemeente er voor te zorgen dat de verwerking met voldoende veiligheidswaarborgen is omkleed. Het beschermingsniveau moet hierbij in verhouding staan tot de te verwerken persoonsgegevens. Zo zullen de verwerkingen die plaatsvinden in het kader van het sociaal domein een hoger beschermingsniveau vereisen dan verwerkingen die plaatsvinden bij het gebruik een afsprakenmodule.

De eerste vraag die steeds beantwoord dient te worden is of de leverancier met persoonsgegevens werkt of niet. De tweede vraag die beantwoord dient te worden is of de relatie tussen een gemeente en een leverancier beoordeeld kan worden als een relatie tussen een verwerkingsverantwoordelijke en een verwerker. Bepalend daarvoor is de bevoegdheid/zeggenschap die de gemeente of de leverancier heeft ten aanzien van de persoonsgegevens die in de eigen organisatie worden verwerkt en worden verstrekt aan de andere organisatie. In de wet wordt dit als volgt omschreven: 'het formeel bevoegd zijn om het doel en middelen te bepalen van de verwerking'. Heeft een gemeente of leverancier zelf de regie over welke persoonsgegevens binnen de organisatie worden verwerkt voor welk doel? Of is sprake van een relatie waarbij bijvoorbeeld de leverancier ten behoeve van de gemeente persoonsgegevens verwerkt?

Gemeente maakt gebruik van ICT-diensten van derden

Een leverancier die een ICT-dienst levert waarbinnen persoonsgegevens worden gebruikt, is normaal wel een verwerker. Denk aan een hosted Customer relationship management (CRM)-systeem, de gemeente slaat de persoonsgegevens op bij de beheerder van het hosted CRM-systeem daarvan. De leverancier is dus een verwerker. Dit geldt ook bij een app-leverancier die persoonsgegevens opslaat op zijn eigen server. Die app is weliswaar on-premise, maar de server is 'gewoon' een dienst.

Gemeente maakt gebruik van SaaS-diensten en hosten data bij derden

Software as a Service (SaaS)-diensten en opslagdiensten vereisen een verwerkersovereenkomst als er persoonsgegevens worden opgeslagen.

Een uitzondering geldt als de dienstverlener niet bij de feitelijke persoonsgegevens kan. Denk aan een versleutelde backupdienst waarbij de gemeente zelf als enige de sleutel heeft. De versleutelde persoonsgegevens gelden dan niet als persoonsgegevens, en is de dienstverlener geen verwerker. Hierbij dient wel opgemerkt te worden dat cryptografische bewerkingen in principe zijn te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens. Dit terrein ontwikkelt zich voortdurend en het is zeer goed mogelijk dat een cryptografische bewerking die in de huidige situatie veilig genoeg is dat over een aantal jaren niet meer is. Bij het toepassen van cryptografische technieken dienen gangbare voorzorgsmaatregelen toegepast te worden, zoals goed ingericht sleutelbeheer en het gebruik van sleutellengten en versleutelingstechnieken die in overeenstemming zijn met de actuele stand van de techniek. Deze voorzorgsmaatregelen dienen regelmatig opnieuw beoordeeld te worden om te zien of deze nog voldoende beveiliging bieden.

Het wordt discutabel als de leverancier er wel bij kan maar dat niet mag. Denk aan een beheerder van de leverancier, waarmee is afgesproken dat de beheerder alleen met expliciete toestemming mappen met persoonsgegevens opent. Als de gemeente dat niet technisch blokkeert, kan de beheerder bij de persoonsgegevens in de mappen. De gemeente dient de beheerder dan te zien als een verwerker. De beheerder is door de gemeente ingehuurd, handelt in opdracht van de gemeente en onder voorwaarden mag de beheerder bij de persoonsgegevens.

Gemeente maakt gebruik van cloudopslag van data

Ook in de situatie dat de gemeente persoonsgegevens opslaat in de cloud is inderdaad een verwerkersovereenkomst vereist. De data die worden opgeslagen dienen dan uiteraard wel persoonsgegevens te zijn.

1 Voor de beantwoording van onderstaande vragen is onder andere gebruik gemaakt van antwoorden die door ICT-jurist Arnoud Engelfriet en juridisch adviseur Philip van der Weijde zijn gegeven naar aanleiding van reacties op artikelen die zijn geplaatst op security.nl en ictrecht.nl. Arnoud Engelfriet is partner en Philip van der Weijde is als juridisch adviseur werkzaam bij het juridisch adviesbureau ICTRecht.

Gemeente laat on-premise software installeren

Laat de gemeente on-premise software installeren waarmee persoonsgegevens zullen worden verwerkt, dan is hierbij niet direct een verwerkersovereenkomst vereist. De leverancier die enkel een softwarepakket levert, verwerkt geen persoonsgegevens. Dat doet de gemeente zelf. Deze leverancier is dus geen verwerker, tenzij de software extern wordt beheerd en niet binnen de eigen gemeentelijk ICT-omgeving. Vaak verzorgt de softwareleverancier echter niet alleen de installatie van de software, maar ook ondersteuning hierop. Daarbij beschikt de softwareleverancier over bijvoorbeeld gebruikersgegevens, wachtwoorden of persoonsgegevens van burgers uit het systeem, maar doet dit op de ICT omgeving van de gemeente. In de situatie waarin de softwareleverancier ondersteuning levert op de software, zal er inderdaad een verwerkersovereenkomst vereist zijn als die partij ook toegang krijgt tot gedeelten van de software waar persoonsgegevens opgeslagen zijn. Dat zal in de meeste gevallen wel aan de orde zijn.

Hoe zit het in het geval er remote verbinding wordt opgezet vanaf de softwareleverancier, naar het netwerk van de gemeente om de werkzaamheden uit te voeren? Ook in de situatie waarin een remote verbinding wordt opgezet, zal dat hetzelfde geval zijn. Criterium is te allen tijde of een derde partij bij de persoonsgegevens kan. Is dat het geval, dan is het belangrijk dat goede afspraken worden vastgelegd met betrekking tot wat de softwareleverancier mag, wie waarvoor verantwoordelijk is en wat bijvoorbeeld moet worden gedaan als de softwareleverancier een datalek veroorzaakt.

Kunnen we de softwareleverancier beschouwen als verwerker wanneer de softwareleverancier enkel verantwoordelijk is voor hosting en beheer van een webportaal die toegang geeft tot persoonsgegevens die in de eigen gemeentelijk omgeving worden opgeslagen op een databaseserver?

Indien de softwareleverancier toegang heeft (of kan hebben) tot de persoonsgegevens opgeslagen op de eigen databaseserver, dan dient de softwareleverancier als verwerker te worden gezien. Het is echter wel de vraag in hoeverre die toegang tot persoonsgegevens onder de beheerwerkzaamheden vallen en of er niet beter maatregelen kunnen worden getroffen die die toegang beperken. Het is hier dus vooral de vraag of de gemeente technisch in staat is de toegang af te schermen? Mocht dat niet het geval zijn, dan is er inderdaad een verwerkersovereenkomst nodig voor wat betreft het uitvoeren van de beheerwerkzaamheden.

Gemeente besteedt personeelsadministratie uit

Wanneer de gemeente de personeelsadministratie uitbesteedt, dan is de gemeente de verwerkingsverantwoordelijke en degene aan wie het is uitbesteed is de verwerker. In dat geval dient er een verwerkersovereenkomst te worden afgesloten.

Ontwikkel- test-, acceptatie- en productie omgeving bij leverancier of gemeente

Stel de leverancier heeft een ontwikkel- en testomgeving, waarin persoonsgegevens opgeslagen zijn. De acceptatie en productie omgeving staan echter bij de gemeente. Er is dus niet echt sprake van cloud of SaaS-dienst, maar het ontwikkelen en testen van de software vindt plaats bij de leverancier.

Bij het ontwikkelen en testen van software zal altijd moeten worden gekeken of er persoonsgegevens worden gebruikt en of die worden verwerkt door iemand anders dan de verwerkingsverantwoordelijke. Test de gemeente de software met persoonsgegevens in een testomgeving van de leverancier, dan zal er zeker een verwerkersovereenkomst vereist zijn. Test de gemeente de software echter met testdata (bijvoorbeeld geanonimiseerd), dan is een verwerkersovereenkomst niet nodig. Wanneer de leverancier de software bij de gemeente komt testen, zal het wel of niet nodig hebben van een verwerkersovereenkomst afhangen van de vraag of de leverancier toegang tot de persoonsgegevens krijgt of dat de persoonsgegevens op een voor de leverancier ontoegankelijke locatie zijn geplaatst. In dat laatste geval is geen verwerkersovereenkomst nodig, in de eerste wel. Het advies is dan ook om bij voorkeur te werken met testdata (bijvoorbeeld geanonimiseerd) en de leverancier geen toegang te geven tot de bij de gemeente aanwezige persoonsgegevens.

Gemeente besteed de verwerking van persoonsgegevens uit een andere gemeente of overheidsinstelling

Het is hierbij de vraag of de gemeente of overheidsinstelling aan wie het werk wordt uitbesteed daadwerkelijk als verwerker optreedt, of de persoonsgegevens voor eigen doeleinden verwerkt. In dat laatste geval is de gemeente of overheidsinstelling namelijk zelf een verwerkingsverantwoordelijke en dient dan ook over een rechtsgeldige grondslag te beschikken. Die grondslag kan bijvoorbeeld gebaseerd zijn op een wettelijke verplichting of noodzakelijk zijn voor een goede vervulling van een publiekrechtelijke taak, maar dat hoeft niet noodzakelijkerwijs het geval te zijn.

Opmerking: Indien de gemeenten of overheidsinstellingen beiden een verwerkingsverantwoordelijke zijn, bestaat er ook nog een verplichting om de betrokkenen te informeren door wie zijn persoonsgegevens worden verwerkt. De betrokkene dient namelijk te weten aan welke partijen zijn persoonsgegevens worden doorgegeven evenals wat de reden daarvan is.

Een online bureau heeft toegang tot het content management systeem (CMS) van een gemeentelijke website. Soms worden er in dat CMS ook persoonsgegevens van burgers opgeslagen, bijvoorbeeld van een ingevuld contactformulier

Deze persoonsgegevens staan opgeslagen bij de hosting provider van de gemeente en in principe kan de hosting provider ook bij die persoonsgegevens. Het online bureau heeft alleen de mogelijkheid van inzage in de persoonsgegevens. Met wie moet de gemeente een verwerkersovereenkomst hebben? Met de hosting provider? Met het online bureau? Of met allebei?

In deze situatie dient de gemeente zowel met het online bureau als de hosting provider een verwerkersovereenkomst te sluiten. Aangezien het online bureau ook toegang heeft tot persoonsgegevens in het CMS systeem, kwalificeert ook zij als verwerker. Het advies is om indien mogelijk bepaalde maatregelen te treffen die ervoor zorgen dat het online bureau niet bij de persoonsgegevens kan, bijvoorbeeld door het CMS systeem tijdelijk af te sluiten. In dat geval hoeft de gemeente ook geen verwerkersovereenkomst te sluiten.

En wat is in het geval van het online bureau het verschil tussen een goede geheimhoudingsverklaring en een verwerkersovereenkomst? Het online bureau kan namelijk niet verantwoordelijk worden gehouden voor de beveiliging van de persoonsgegevens, omdat het systeem eigendom is van en beheerd wordt door de hosting provider en niet door het online bureau.

Met het online bureau dient de gemeente ook afspraken te maken omtrent geheimhouding. Zo kan het online bureau bijvoorbeeld toegang krijgen tot informatie over de bedrijfsvoering of de werking van bepaalde software. De geheimhoudingsovereenkomst is echter niet de plek om afspraken over de omgang met persoonsgegevens vast te leggen. De wet schrijft ook voor dat afspraken over de verwerking van persoonsgegevens in een overeenkomst dienen te worden vastgelegd. Wel is het weer gebruikelijk om in een verwerkersovereenkomst afspraken over geheimhouding vast te leggen.

Een cloudleverancier van fiscale software (daarin staat dus onder andere NAW, BSN en Geb. datum) beweert dat verwerkersovereenkomst opnemen in de Algemene Voorwaarden de norm is. De verantwoordelijke is het daar niet mee eens: een verwerkersovereenkomst stemt men in onderling overleg af en daar tekenen de partijen voor. Het eenzijdig aanpassen van de Algemene Voorwaarden is daar geen sprake van (en wordt ook niet ondertekend door beide partijen).

Door bepalingen over de verwerkersovereenkomst in de algemene voorwaarden op te nemen, voldoet de cloudleverancier aan zijn verplichtingen. De verwerkingsverantwoordelijke is echter de partij die op basis van de wet moet zorgen voor een verwerkersovereenkomst. Dit moet op basis van de Memorie van Toelichting bij de Wbp een afzonderlijke overeenkomst zijn. De tekst luidt als volgt: "De overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker moet naar zijn aard betrekking hebben op de gegevensverwerking. Het contract mag niet betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is". Op de website van de AP staat dit nader beschreven.[1]

Wie zijn de verwerkingsverantwoordelijke en verwerker in het sociaal domein bijvoorbeeld Wmo en Jeugdwet?

Voor hun eigen werk (hulp) zijn hulpaanbieders zelf de verwerkingsverantwoordelijke. Bijvoorbeeld voor:

- De Wet maatschappelijke ondersteuning 2015 (Wmo), de aanbieders van maatwerkvoorzieningen en van algemene voorzieningen en
- De Jeugdwet, de aanbieders van individuele voorzieningen en van algemene voorzieningen.

Net zoals gecertificeerde instellingen en de Raad voor de Kinderbescherming (RvdK) zelf de verwerkingsverantwoordelijke zijn bij de Jeugdwet en het Advies- en Meldpunt Huiselijk geweld en Kindermishandeling (AMHK) zelf de verwerkingsverantwoordelijke is bij de Wmo.[2, 3]

In de relatie gemeente (als opdrachtgever / financier) - hulpaanbieder is de hulpaanbieder bij hulp dus geen verwerker voor de gemeente. Daarop is er één uitzondering en dat is alleen als de gemeente zelf expliciet als hulpaanbieder optreedt (wat mogelijk is) en vervolgens die gemeentelijke hulp uitbesteed (wat merkwaardig is want waarom zou de gemeente bij toch uitbesteden van de hulp er dan als gemeente eerst voor kiezen om zelf aanbieder te zijn?). Dan is de gemeente de verwerkingsverantwoordelijke. Maar dit is toch meer een uitzondering.

Een andere situatie is er als de gemeente de toeleidingstaken van de gemeente (bijvoorbeeld de uitvoering van artikel 2.3 of artikel 2.4 Jeugdwet of de uitvoering van de artikelen 2.3.4, 2.3.5 en 2.3.6 Wmo) uitbesteed aan aanbieders. Dit is mogelijk en gebeurt ook vaak. Dan treden de aanbieders niet als aanbieders van hulp op, maar als organisaties die namens de gemeente de toeleiding doen. Dan is de gemeente (college B&W) de verwerkingsverantwoordelijke en zijn de aanbieders (lees toeleidende organisaties) verwerker.

Er kunnen zich dus drie situaties voordoen:

1. de hulpaanbieder die hulp verleent;
2. de gemeente die expliciet zelf hulpaanbieder wordt;
3. organisaties waaraan gemeentelijke toeleidingstaken zijn uitbesteed.

1 https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-2-voorwaarden-voor-de-rechtmatigheid-van-de-verwerking-v-25

2 Zie bijvoorbeeld de artikelen 5.1.2 lid 3, en 5.1.6 lid 1 Wmo. De aanwijzing van verwerkingsverantwoordelijke in artikel 5.1.2 lid 3 Wmo heeft, juridisch bezien, tot gevolg dat het bieden van hulp door derden als bedoeld in artikel 2.6.4 Wmo (die derden zijn de aanbieders) NIET als resultaat heeft dat bijvoorbeeld de gemeente verwerkingsverantwoordelijke zou zijn. Overigens is artikel 2.6.4 Wmo vooral een aanbestedingsregeling en niet bedoeld als Wbp-regeling.

3 Helemaal afhankelijk van de situatie geldt er voor de aanbieder of de medewerkers van de aanbieder een specifieke geheimhouding op grond van de Jeugdwet, de Wmo of de Wet geneeskundige behandelovereenkomst (WGBO)

Wie de verwerkingsverantwoordelijke is verschilt per situatie. Dat maakt het wellicht wel wat verwarrend voor de praktijk, zeker in gevallen waarin een organisatie zowel de gemeentelijke toeleiding doet als ook zelf hulp verleend. Bij de vraag of het een verwerkingsverantwoordelijke of een verwerker is staat dan ook de taak die uitgevoerd wordt centraal en pas daarna welke organisatie die taak uitvoert.

Samengevat:

- Artikel 2.6.3 Wmo dan gaat het niet om hulp, maar gaat het om de gemeentelijke toeleiding van onder andere artikel 2.3.5 Wmo en is de gemeente de verwerkingserantwoordelijke en de organisatie die de toeleiding feitelijk uitvoert verwerker.
- Artikel 2.6.4 Wmo dan gaat het om de hulp zelf en zijn de hulpaanbieders de verwerkingsverantwoordelijke.

Is er voor de gegevensuitwisseling tussen een gemeente en een zorgverlener, in het kader van de uitvoering van een zorgverleningsovereenkomst, een verwerkersovereenkomst nodig?

De eerste vraag die hierbij beantwoord dient te worden is of de relatie tussen een gemeente en een zorgaanbieder wel beoordeeld kan worden als een relatie tussen een verwerkingsverantwoordelijke en een verwerker. Bepalend daarvoor is de bevoegdheid/zeggenschap die de gemeente of de zorgaanbieder heeft ten aanzien van de persoonsgegevens die in de eigen organisatie worden verwerkt en worden verstrekt aan de andere organisatie (in de Wbp wordt dit als volgt omschreven: de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen). Hierbij kunnen de volgende twee situaties worden onderkend:

1. Heeft een gemeente of zorgaanbieder zelf de regie over welke persoonsgegevens binnen de organisatie worden verwerkt voor welk doel?
2. Is er sprake van een relatie waarbij bijvoorbeeld de zorgaanbieder ten behoeve van de gemeente persoonsgegevens verwerkt?

De zorgaanbieder zou dan moeten handelen naar de instructies en onder verantwoordelijkheid van de gemeente bij het verwerken van zijn persoonsgegevens. Daar is natuurlijk geen sprake van. De dienstverlening van de zorgaanbieder zou dan gericht moeten zijn op het uitvoeren van een bepaalde verwerking van persoonsgegevens ten behoeve van de gemeente (vergelijkbaar met een bedrijf dat in opdracht van een ander bedrijf de salarisadministratie van dat bedrijf uitvoert). Ook daar is geen sprake van bij een zorgverlener. Diens dienstverlening is immers gericht op het verlenen van zorg. Een zorgaanbieder heeft daarbij zelf de zeggenschap en verantwoordelijkheid over welke persoonsgegevens van cliënten worden vastgelegd en gedeeld met gemeenten.

We hebben hier te maken met partijen die ten opzichte van elkaar verwerkingsverantwoordelijke zijn. Er is dus geen verwerkersovereenkomst nodig. Wel wordt aanbevolen om op een andere wijze afspraken te maken over de zorgvuldige omgang met persoonsgegevens waaronder ook afspraken over welke persoonsgegevens worden gedeeld et cetera. Dit is wettelijk niet verplicht.

DEZE FACTSHEET IS OPGESTELD IN SAMENWERKING MET DE VERENIGING NEDERLANDSE GEMEENTEN.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.