

Verwerker en verwerkingsverantwoordelijke

whitepaper

Inhoudstabel

Inhoudstabel	2
Doel	4
Wettelijke verplichtingen.....	5
Definities	5
Wettelijke verplichting: de verwerkersovereenkomst.	5
Plan van aanpak	7
Verwerkingsverantwoordelijke of verwerker?	8
Vormgeving van de verwerkersovereenkomst.....	10
Verskil geheimhoudingsverklaring en verwerkersovereenkomst	10
De verwerkersovereenkomst en de algemene voorwaarden	10
Afspraken maken	10
Verwerkingsverantwoordelijke – verwerker	10
Twee verwerkingsverantwoordelijken	10
Voorbeeldsituaties wanneer wel en wanneer geen verwerkersovereenkomst.....	11
Dienst Gezinszorg maakt gebruik van ICT diensten van derden.....	11
Dienst Gezinszorg maakt gebruik van SaaS diensten en host data bij derden	11
Dienst Gezinszorg maakt gebruik van cloudopslag van data.....	11
Dienst Gezinszorg laat on-premise software installeren	11
Dienst Gezinszorg besteedt personeelsadministratie uit	12
Ontwikkel-, test- en/of acceptatie omgevingen bij leverancier	12
Dienst Gezinszorg besteedt de verwerking van persoonsgegevens uit aan een andere Dienst (Gezinszorg, VDAB, ...).....	12
Gegevensuitwisseling tussen Dienst Gezinszorg en zorgverlener	12
Gegevensuitwisseling tussen Dienst Gezinszorg en de boekhouder.....	13
Referenties.....	14

Aanpassingen historiek

Datum	Reden voor de aanpassing	Auteur	Versie
20/09/2017	Eerste versie	Kristel Van Aken, veiligheidsadviseur VVDG	1.0

Doel

Organisaties worden geconfronteerd met een aantal nieuwe wettelijke verplichtingen door de komst van de nieuwe privacywet – de Algemene Verordening Gegevensverwerking of kortweg AVG. Eén van die verplichtingen houdt in dat de uitvoering van verwerkingen van persoonsgegevens door een derde partij ten behoeve van een organisatie, moet geregeld worden in een overeenkomst, namelijk de verwerkersovereenkomst. Die derde partij wordt in de AVG *de verwerker* genoemd, terwijl de organisatie zelf de *verwerkersverantwoordelijke* is.

Er is nogal wat onduidelijkheid over wie nu juist onder de noemer ‘verwerker’ valt. Gaat het hier over elke derde partij waarmee gegevens worden uitgewisseld? Wie is dat dan concreet? Dit document beoogt hier meer duidelijkheid in te scheppen, specifiek voor de Diensten Gezinszorg.

Dit document moet beschouwd worden als leidraad, gebaseerd op onderzoekswerk en gesprekken met experts; het biedt geen juridisch advies.

Wettelijke verplichtingen

Definities

Iedereen heeft recht op bescherming van zijn of haar persoonsgegevens. Dit wordt vanaf 25 mei 2018 concreet gemaakt door de AVG. Deze AVG vervangt de huidige Belgische 'Wet ter Bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens'. Dat betekent dat vanaf die datum er één privacywet geldt in de hele Europese Economische Ruimte.

Het is dan ook hoog tijd om actief aan de slag te gaan om de privacy van personen te waarborgen, zowel intern als in de samenwerking met toeleveranciers, dienstverleners en andere externe partijen. Diensten Gezinszorg hebben steeds vaker een deel van hun persoonsgegevens buiten de deur staan bij een derde partij of maken gebruik van derden die in hun opdracht persoonsgegevens verwerkt. Deze derde partijen (die dus in opdracht werken van een Dienst Gezinszorg) worden verwerkers genoemd, de Diensten Gezinszorg is dan de verwerkingsverantwoordelijke.

De AVG definieert deze begrippen als volgt:

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.'

Wettelijke verplichting: de verwerkersovereenkomst.

Volgens artikel 28 van de AVG moet de uitvoering van verwerkingen door een verwerker geregeld worden in een overeenkomst, de verwerkersovereenkomst genaamd. De overeenkomst moet schriftelijk of in elektronische vorm zijn vastgelegd. Bindende afspraken tussen verwerkingsverantwoordelijke en verwerker kunnen ook blijken uit andere rechtshandelingen mits voldaan is aan de vereisten.

In de praktijk betekent dit voor de Diensten Gezinszorg dat zij een verwerkersovereenkomst moeten hebben met elke betrokken verwerker, d.w.z. met elke derde partij die ten hare behoefte persoonsgegevens verwerkt (in brede zin van het woord – zie ook verder in dit document).

De verwerkersovereenkomst geeft tevens de keten in het proces van verwerking tussen de verwerkingsverantwoordelijke, verwerkers en eventuele sub-verwerkers weer en geeft inzicht in de verdeling van verantwoordelijkheden en aansprakelijkheden. De kern hierbij is dat de verwerkingsverantwoordelijke verantwoordelijk én aansprakelijk is voor de gegevensverwerking. 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 veiligheidsmaatregelen bieden opdat de verwerking aan de vereisten voldoen en de bescherming van de rechten van de betrokkene is gewaarborgd.

Merk op dat zowel verwerkingsverantwoordelijke als verwerker nog andere wettelijke verplichtingen hebben volgens de AVG, maar deze vallen buiten de scope van dit document.

Plan van aanpak

Best wordt begonnen met het maken van een overzicht van alle derde partijen waar persoonsgegevens mee worden uitgewisseld. Uit die lijst kan men dan een selectie maken van alle derde partijen die in opdracht van de Dienst Gezinszorg diensten verlenen die betrekking hebben op de verwerking van persoonsgegevens. Dit zijn dan verwerkers.

Merk op dat de andere derde partijen waarmee persoonsgegevens worden uitgewisseld, maar die geen verwerking doen in opdracht en onder instructies van de verwerkingsverantwoordelijke, geen verwerkers zijn. Dit gegeven wordt verder uitgewerkt in volgend hoofdstuk.

Vervolgens kan worden nagegaan of met alle verwerkers afspraken zijn gemaakt in een verwerkersovereenkomst en of deze aangepast moeten worden aan de regels van de AVG.

De Dienst Gezinszorg en de verwerker moeten samen afspraken maken over taken en verantwoordelijkheden in het kader van veilige verwerking van persoonsgegevens. De manier waarop dit geregeld wordt moet altijd voldoen aan de wet. Daarnaast moet De Dienst Gezinszorg met de verwerker in overleg over de invulling van de afspraken rond de veilige verwerking van persoonsgegevens. Beide partijen leggen vervolgens al deze afspraken schriftelijk vast in de verwerkersovereenkomst.

Er moet minstens over volgende wettelijke verplichtingen afspraken worden gemaakt:

- Persoonsgegevens worden uitsluitend verwerkt volgens de instructies van de Dienst Gezinszorg.
- De waarborgen inzake vertrouwelijkheid.
- De waarborgen die de verwerker biedt ten aanzien van technische en organisatorische maatregelen en de manier waarop de Dienst Gezinszorg dit kan controleren.
- De wijze waarop de Dienst Gezinszorg wordt geïnformeerd bij een veiligheidsincident en de informatie die hierover wordt bijgehouden.
- Teruggave of vernietiging van de gegevens bij einde van de overeenkomst.
- 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 Dienst Gezinszorg als de verwerker belang heeft bij redelijke eisen. De Dienst Gezinszorg moet zijn verantwoordelijkheid kunnen nemen bij de uitbesteding van verwerkingen van persoonsgegevens. Tegelijk moet de verwerker een gezonde bedrijfsvoering kun uitoefenen.

Verwerkingsverantwoordelijke of verwerker?

Verwerken is een ruim begrip, als een derde partij bij de door de Dienst Gezinszorg verzamelde persoonsgegevens kan, wordt dit voor de wet gezien als een verwerken van persoonsgegevens en is de AVG van kracht. De derde partij hoeft echter niet altijd een verwerker te zijn maar kan zelf ook een verwerkingsverantwoordelijke zijn.

Wanneer de Dienst Gezinszorg de persoonsgegevens laat verwerken door een derde partij in opdracht en onder instructies van de Dienst Gezinszorg, is de derde partij een verwerker. Het juridische criterium van 'opdracht' is of de Dienst Gezinszorg het doel, en de middelen van het verwerken en over welke persoonsgegevens het gaat, vaststelt. Ook is het belangrijk te weten dat de persoonsgegevens enkel in opdracht en volgens aanwijzingen die zijn opgenomen in de verwerkersovereenkomst van de verwerkingsverantwoordelijke mogen worden verwerkt. De verwerker mag de persoonsgegevens niet op eigen gezag gaan verwerken. De verwerkingsverantwoordelijke dient na te gaan of dit ook zo gebeurt.

Merk op dat de AVG het vastleggen van de middelen bij de verwerkingsverantwoordelijke legt. Wat er precies onder 'middelen' wordt bedoeld, is niet bij wet bepaald. Hoe zit het bijvoorbeeld met het uitbesteden van een verwerking naar een software dienstverlener, waarbij de dienstverlener zelf de infrastructuur, de ondersteunende hardware/software en andere technische maatregelen bepaalt? Volgens de aanbevelingen van de 'working party 29' van de Europese Commissie, wordt in dit geval wel degelijk de dienstverlener beschouwd als een verwerker, mits hij in opdracht van de verwerkingsverantwoordelijke werkt. De verwerker kan dus in beperkte mate een zekere vrijheid hebben bij het mede bepalen van de technische en organisatorische 'middelen' van de verwerking.

Wanneer is nu sprake van een verwerker?

De eerste vraag die steeds moet worden beantwoord, is of de derde partij met persoonsgegevens werkt of niet. De tweede vraag die moet worden beantwoord is of de relatie tussen de Dienst Gezinszorg en de derde partij beoordeeld kan worden als een relatie tussen een verwerkingsverantwoordelijke en een verwerker. Bepalend hiervoor is de bevoegdheid/zeggenschap die de Dienst Gezinszorg of de derde partij heeft ten aanzien van de persoonsgegevens die in de eigen organisatie worden verwerkt en worden verstrekt aan de andere organisatie. Heeft de Dienst Gezinszorg of de derde partij de regie over welke persoonsgegevens worden verwerkt en voor welk doel? Of is er sprake van een relatie waar bijvoorbeeld een leverancier persoonsgegevens verwerkt ten behoeve van de Dienst Gezinszorg?

Een andere manier om de zaak te bekijken, is de volgende: een verwerker komt enkel ter sprake door een beslissing van de verwerkingsverantwoordelijke. Deze beslist autonoom om ofwel de verwerking in-huis uit te voeren ofwel om (deel van) de verwerking uit te besteden. Elke andere relatie, waarbij de andere partij autonoom beslist om persoonsgegevens te verwerken, al zijn die gegevens afkomstig van een andere organisatie, is een relatie tussen twee verwerkingsverantwoordelijken.

Het is perfect mogelijk dat de derde partij zowel verwerkingsverantwoordelijke als verwerker is. Alles hangt af van de manier waarop de verwerking aan de derde partij wordt opgedragen. Indien er duidelijke en gedetailleerde instructies gegeven worden omtrent (een deel van) de verwerking, is er sprake van verwerkingsverantwoordelijke – verwerker relatie en moet een verwerkersovereenkomst

voor (dat deel van) de verwerking opgesteld worden. Maar het is mogelijk dat de verwerker zelf een verwerking opstart, waarbij het zelf het doel en de middelen definieert. Voor dit deel van de verwerking is die verwerker dan zelf verwerkingsverantwoordelijke.

Kort samengevat:

1. Is er sprake van een derde partij die (potentieel) toegang heeft tot persoonsgegevens?

Neen? Dan stopt het verhaal hier.

Ja? Dan ga naar 2

2. Geeft de Dienst Gezinszorg instructies aan de derde partij over welke persoonsgegevens verwerkt worden, met welk doel en welke middelen?

Neen? Dan overweeg het opstellen van een informatie uitwisselingsovereenkomst (hierover meer verder in dit document).

Ja? Dan stel een verwerkersovereenkomst op rond deze verwerking.

Enkele criteria om tot een juiste kwalificatie te komen:

- Niveau van vooraf gegeven instructies gegeven door de verwerkingsverantwoordelijke, waardoor er weinig vrijheid overblijft voor de derde partij (die dan beschouwd wordt als verwerker);
- Opvolging en monitoring van de uitvoering van de dienstverlening: continue supervisie van conformiteit met de opgelegde instructies en de contractuele voorwaarden door de verwerkingsverantwoordelijke;
- Visibiliteit gegeven door de verwerkingsverantwoordelijke ten aanzien van de betrokkenen (wiens persoonsgegevens verwerkt worden) en de verwachtingen van de betrokkenen op basis van deze visibiliteit.

Vormgeving van de verwerkersovereenkomst

Verschil geheimhoudingsverklaring en verwerkersovereenkomst

Een geheimhoudingsverklaring is een afspraak tussen partijen om bepaalde informatie niet zomaar vrij te geven. Het gaat hier dus over afspraken rond geheimhouding, maar de scope van de geheimhoudingsverklaring kan verder gaan dan enkel persoonsgegevens. Afhankelijk van de bepalingen in het document kan het immers ook over bedrijfsgebonden informatie gaan.

De geheimhoudingsverklaring is echter niet de plek om afspraken over omgang met persoonsgegevens vast te leggen. De AVG schrijft specifiek voor welke afspraken over de verwerking van persoonsgegevens in een overeenkomst dienen te worden vastgelegd. Wel is het gebruikelijk om in een verwerkersovereenkomst afspraken over geheimhouding rond persoonsgegevens vast te leggen.

De verwerkersovereenkomst en de algemene voorwaarden

Volgens de AVG moet de verwerkersovereenkomst opgesteld worden door de verwerkingsverantwoordelijke. Deze overeenkomst moet een afzonderlijk document zijn.

Het opnemen van bepalingen van de verwerkersovereenkomst in de algemene voorwaarden van de verwerker voldoet dus niet omdat dit eenzijdig door de verwerker gebeurt.

Afspraken maken

Verwerkingsverantwoordelijke – verwerker

Indien er sprake is van een relatie verwerkingsverantwoordelijke – verwerker, moet de verwerkingsverantwoordelijke zorgen voor een verwerkersovereenkomst met de verwerker. De bepalingen in deze overeenkomst zijn wettelijk vastgelegd, namelijk in de AVG.

Twee verwerkingsverantwoordelijken

Maar wat als er geoordeeld wordt dat er geen sprake is van een verwerkingsverantwoordelijke – verwerker relatie? In dit geval worden beide partijen aanzien als verwerkingsverantwoordelijke en is er geen verwerkersovereenkomst nodig.

De AVG specificeert niet welke contractuele afspraken gedocumenteerd moeten worden in een relatie tussen twee verwerkingsverantwoordelijken. Desondanks is het aan te bevelen afspraken te maken over zorgvuldige omgang met persoonsgegevens, bijvoorbeeld via een informatie uitwisselingsovereenkomst. Zulke overeenkomst bevat details over welke informatie gedeeld wordt, afspraken rond geheimhouding, rond wederzijdse mededeling ingeval van inbreuken, enz. Deze overeenkomst is echter geen AVG verplichting.

Voorbeeldsituaties wanneer wel en wanneer geen verwerkersovereenkomst.

Dienst Gezinszorg maakt gebruik van ICT diensten van derden

Een leverancier die een ICT dienst levert waarbinnen persoonsgegevens voorkomen, is normaal een verwerker. De leverancier is dan een verwerker. Dit geldt ook bij een software leverancier die persoonsgegevens opslaat op zijn eigen server. In dit scenario is de software weliswaar on-premise bij de Dienst Gezinszorg, maar de server is gewoon een dienst.

Om als verwerker aanzien te worden, volstaat het dus dat een leverancier of beheerder *mogelijk* toegang heeft tot de persoonsgegevens waarvoor de Dienst Gezinszorg verantwoordelijk is, ook al doet de leverancier of beheerder strikt genomen geen acties rond deze persoonsgegevens (acties zoals aanmaken, bijwerken of verwijderen).

Dienst Gezinszorg maakt gebruik van SaaS diensten en host data bij derden

SaaS diensten en opslagdiensten vereisen een verwerkersovereenkomst als er persoonsgegevens worden opgeslagen.

Een uitzondering geldt als de dienstverlener niet bij de feitelijke persoonsgegevens kan, bijvoorbeeld omdat deze versleuteld zijn waarbij de Dienst Gezinszorg als enige de encryptie sleutel heeft.

Heel anders is de situatie waarbij de leverancier wel bij de data kan maar niet mag, bijvoorbeeld omdat de leverancier beheerder is van de onderliggende infrastructuur en de data niet versleuteld is of indien de data versleuteld is maar de encryptiesleutel beheerd wordt door de leverancier. De Dienst Gezinszorg dient de leverancier dan te zien als een verwerker. De leverancier is door de Dienst Gezinszorg ingehuurd, handelt in opdracht van de Dienst.

Dienst Gezinszorg maakt gebruik van cloudopslag van data

Ook in de situatie dat de Dienst Gezinszorg persoonsgegevens opslaat in de cloud vereist een verwerkersovereenkomst, tenzij deze gegevens voldoende afgeschermd zijn van de cloud provider, bijvoorbeeld door encryptie waarbij de encryptiesleutel *niet* beheerd wordt door de cloud provider.

Dienst Gezinszorg laat on-premise software installeren

Laat de Dienst Gezinszorg in-premise software installeren waarmee persoonsgegevens worden verwerkt, dan is hierbij niet altijd een verwerkersovereenkomst nodig. De leverancier die enkel een software pakket levert, verwerkt geen persoonsgegevens op voorwaarde dat deze leverancier op geen enkel ogenblik aan de persoonsgegevens kan.

Maar als de leverancier de software beheert en ondersteuning levert, waarbij toegang tot persoonsgegevens mogelijk is, dan moet de leverancier wel aanzien worden als verwerker en is een verwerkersovereenkomst nodig. Dit is evenzeer nodig indien er sprake is van beheer op afstand, waarbij een remote verbinding wordt opgezet tussen de leverancier en het netwerk om de werkzaamheden uit te voeren.

Criterium is dus altijd of een derde partij toegang zou kunnen hebben tot de persoonsgegevens waarvoor de Dienst Gezinszorg de verwerkingsverantwoordelijke is.

Dienst Gezinszorg besteedt personeelsadministratie uit

Wanneer de Dienst Gezinszorg de personeelsadministratie uitbesteedt bijvoorbeeld aan een sociaal secretariaat dan is de Dienst de verwerkingsverantwoordelijke en degene aan wie het is uitbesteed de verwerker en is dus een verwerkersovereenkomst nodig.

Ontwikkel-, test- en/of acceptatie omgevingen bij leverancier

Stel de leverancier heeft een ontwikkel- en testomgeving waarin persoonsgegevens opgeslagen zijn. De acceptatie- en productie omgeving staan bij de Dienst Gezinszorg. Er is niet echt sprake van een cloud of SaaS dienst, maar het ontwikkelen en testen van software vindt plaats bij de leverancier (of een andere derde partij, bijvoorbeeld aan andere Dienst Gezinszorg).

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 Dienst Gezinszorg de software met persoonsgegevens in een testomgeving van de leverancier dan is een verwerkersovereenkomst vereist. Test de Dienst Gezinszorg de software met testdata (geanonimiseerd) dan is een verwerkersovereenkomst niet nodig. Wanneer de leverancier de software bij de Dienst Gezinszorg komt testen, zal het wel of niet nodig hebben van verwerkersovereenkomst afhangen van de vraag of de leverancier toegang tot de persoonsgegevens krijgt of niet.

Dienst Gezinszorg besteedt de verwerking van persoonsgegevens uit aan een andere Dienst (Gezinszorg, VDAB, ...)

Het is hierbij de vraag of de Dienst aan wie het werk wordt uitbesteed daadwerkelijk als verwerker optreedt, dus op instructies van de Dienst Gezinszorg, of de persoonsgegevens voor eigen doeleinden verwerkt. In dit laatste geval zijn beide Diensten verwerkingsverantwoordelijken en dienen dan ook over een rechtsgeldige grondslag te beschikken.

Gegevensuitwisseling tussen Dienst Gezinszorg en zorgverlener

Om te beoordelen of er in dit geval sprake is van een verwerker, moet de relatie tussen de Dienst Gezinszorg en de zorgverlener beoordeeld worden. Bepalend hiervoor is de bevoegdheid/zeggenschap die de Dienst Gezinszorg of de zorgverlener heeft ten opzichte van de persoonsgegevens. Hierbij kunnen twee situaties zich voordoen:

1. Heeft de Dienst Gezinszorg of de zorgverlener de regie over welke persoonsgegevens binnen de organisatie worden verwerkt en voor welk doel?
2. Is er sprake van een relatie waarbij de zorgverlener louter ten behoeve van de Dienst Gezinszorg persoonsgegevens verwerkt?

In dit laatste geval handelt de zorgverlener naar de instructies en onder verantwoordelijkheid van de Dienst Gezinszorg. De dienstverlening van de zorgverlener is dan gericht op het uitvoeren van een bepaalde verwerking van persoonsgegevens ten behoeve van de Dienst Gezinszorg. Er moet in deze situatie een verwerkersovereenkomst opgesteld worden.

Indien de zorgverlener zelf de zeggenschap en verantwoordelijkheid heeft over welke persoonsgegevens van cliënten worden vastgelegd en gedeeld met de Dienst Gezinszorg, moet de zorgverlener zelf niet aanzien worden als een verwerker: er is sprake van twee partijen die ten opzichte van elkaar verwerkingsverantwoordelijke zijn.

Gegevensuitwisseling tussen Dienst Gezinszorg en de boekhouder

Of een boekhouder beschouwd moet worden als verwerkingsverantwoordelijke of verwerker, hangt nauw samen met de context waarin hij/zij werkt. Indien de boekhouder diensten verleent op basis van generieke instructies (bijvoorbeeld 'maak mijn belastingaangifte in orde'), dan is deze boekhouder een verwerkingsverantwoordelijke.

Als de boekhouder wordt aangesteld door de organisatie met nauwgezette instructies en onder controle van bijvoorbeeld de financieel directeur, bijvoorbeeld om audits uit te voeren, dan moet hij/zij beschouwd worden als verwerker.

In het meest voorkomende geval zal onze boekhouder echter beschouwd moeten worden als verwerkingsverantwoordelijke en is een verwerkersovereenkomst niet nodig. Het kan echter niet genoeg herhaald worden dat in dit geval een informatie uitwisselingsovereenkomst wel raadzaam is.

Referenties

AVG: algemene verordening gegevensbescherming:

<https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0>

Article 29 Data Protection Working Party opinion 1/2010 on the concepts of 'controller' and 'processor': http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf