Factsheet Deel 1:

Omgaan met persoonsgegevens door zorgaanbieders: Algemene Verordening Gegevensbescherming (AVG)

Oktober 2017

Factsheet deel 1: Omgaan met persoonsgegevens door zorgaanbieders: Algemene Verordening Gegevensbescherming (AVG)

Iedere zorgaanbieder verwerkt persoonsgegevens. Op dit moment gelden hiervoor nog de privacy verplichtingen uit de Wet bescherming persoonsgegevens (**Wbp**). Vanaf 25 mei 2018 wordt de Wbp vervangen door de Algemene Verordening Gegevensbescherming (**AVG**). De AVG kent een aantal dezelfde uitgangspunten en begrippen als de Wbp maar introduceert ook nieuwe verplichtingen voor u als de verwerkingsverantwoordelijke en de organisaties die u als verwerker van persoonsgegevens (onder de Wbp: bewerker) inschakelt. In deze Factsheet komen de belangrijkste verplichtingen uit de AVG aan bod.

In december 2014 publiceerde de VGN een Factsheet over het omgaan met persoonsgegevens met het oog op de Wbp, de Wet maatschappelijke ondersteuning 2015 (**Wmo 2015**) en de Jeugdwet: Factsheet 2014. Gezien de veranderingen in onder andere de privacy wetgeving, hebben wij de Factsheet 2014 vernieuwd en bestaat deze nu uit twee delen:

1 Factsheet omgaan met persoonsgegevens: Algemene Verordening Gegevensbescherming (AVG)
2 Factsheet omgaan met persoonsgegevens: Wmo 2015, Jeugdwet en Wet langdurige zorg (**Wlz**)

Deze Factsheet AVG bespreekt op hoofdlijnen de privacy regelgeving die van toepassing is op zorgaanbieders. De Factsheet AVG begint met de belangrijkste begrippen uit de AVG en zet daarna de belangrijkste verplichtingen op een rij. Aan het einde van deze Factsheet AVG vindt u een stappenplan met acties die u kunt nemen zodat uw organisatie kan voldoen aan de AVG.

1 Verwerken van persoonsgegevens - begrippen

1.1 Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn tot een individu, de betrokkene.[1] Bij de persoonsgegevens die u als zorgaanbieder verwerkt moet u in de eerste plaats denken aan cliëntgegevens zoals de naam van de cliënt, (e-mail) adres, telefoonnummer, informatie over bepaalde beperkingen of aandoeningen en gegevens van familieleden van de cliënt. U zult daarnaast, evenals andere werkgevers, bijvoorbeeld ook persoonsgegevens van uw werknemers verwerken, alsmede contactgegevens van dienstverleners.

1.2 U heeft te maken met privacy regels zodra u persoonsgegevens "verwerkt" of laat "verwerken". Dit doet u bijvoorbeeld als u de persoonsgegevens bijwerkt, verzamelt, vastlegt, ordent en bewaart, maar ook als u deze alleen raadpleegt of zelfs vernietigt.[2] Het verstrekken van de cliëntgegevens aan gemeenten en zorgkantoren is eveneens een verwerkingshandeling, waarbij u de verplichtingen uit hoofde van de

[1] Art. 1 sub a Wbp; Art. 4 lid 1 AVG.

[2] Art. 1 sub b Wbp; Art. 4 lid 2 AVG.

Wbp en de AVG moet naleven, alsmede specifieke verplichtingen zoals onder andere beschreven in de Wmo 2015, de Jeugdwet en de Wlz.[3]

1.3 De persoonsgegevens die u verwerkt zullen deels "gewone" persoonsgegevens zijn zoals namen, (e-mail) adressen en telefoonnummers. Deels zult u bijzondere persoonsgegevens verwerken waarvoor strengere regels gelden dan voor gewone persoonsgegevens.[4] Bijzondere persoonsgegevens zijn onder andere gezondheidsgegevens en de AVG heeft hier nog genetische gegevens en biometrische gegevens aan toegevoegd. Een Burgerservicenummer (**BSN**) is volgens de AVG geen bijzonder persoonsgegeven. Omdat een BSN wel van gevoelige aard is en er bij onrechtmatige verwerking risico bestaat op fraude gelden ten aanzien van het BSN aparte regels bovenop de AVG, zoals onder andere vastgelegd in de Wet cliëntenrechten bij elektronische verwerking van gegevens.[5]

1.4 De AVG maakt onderscheid tussen de verwerkingsverantwoordelijke en de verwerker van persoonsgegevens:

1.4.1 De verwerkingsverantwoordelijke is degene die (al dan niet samen met een ander) formeel-juridisch zeggenschap over de verwerking heeft en het doel en de middelen voor de verwerking vaststelt.[6] De verwerkingsverantwoordelijke bepaalt het 'hoe en waarom' van de gegevensverwerking. Het is niet noodzakelijk dat de verwerkings-verantwoordelijke ook zelf persoonsgegevens verwerkt en onder zich heeft.

In de meeste gevallen zal u als zorgaanbieder als verwerkingsverantwoordelijke zijn aan te merken, denk bijvoorbeeld aan uw cliëntenadministratie en uw personeelsadministratie: u bepaalt zelf hoe u uw administratie inricht en wat u met de persoonsgegevens doet.

1.4.2 De verwerker verwerkt persoonsgegevens uitsluitend ten behoeve van en in opdracht van de verwerkingsverantwoordelijke.[7] De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken.

Zorgaanbieders die als verwerkingsverantwoordelijken persoonsgegevens verwerken maken doorgaans gebruik van de diensten van derden, denk aan een IT leverancier of een uitvoerder voor salarisadministratie.

---

3 Zie ook Factsheet omgaan met persoonsgegevens: Wmo 2015, Jeugdwet en Wlz.

4 Art. 16-21 en art. 23 Wbp; Art. 9 AVG.

5 In de Wet cliëntenrechten bij elektronische verwerking van gegevens worden specifieke regels neergelegd in art. II. In andere wetten, zoals de Wmo 2015, de Jeugdwet en de Wlz zijn ook specifieke bepalingen neergelegd over het gebruik van een BSN. Hier is meer over te lezen in de 'Factsheet omgaan met persoonsgegevens: de Wmo 2015, de Jeugdwet en de Wet langdurige zorg'. Naar verwachting zal ook in de Uitvoeringswet AVG een bepaling worden opgenomen ten aanzien van de verwerking van een BSN. Bij het opstellen van deze Factsheet is de Uitvoeringswet AVG nog niet aangenomen.

6 Art. 1 sub d Wbp; Art. 4 lid 7 AVG.

7 Art. 1 sub e Wbp; Art. 4 lid 8 AVG.

Wanneer die partij namens u persoonsgegevens verwerkt, en niet ook zelf bepaalt wat met de persoonsgegevens gebeurt, dan is dit een verwerker.

1.5 Het grootste deel van de verplichtingen uit de AVG rusten op u als verwerkingsverantwoordelijke. Deze hebben wij verder uitgewerkt in paragraaf 2. Wat nieuw is onder de AVG is dat nu ook de verwerker die u inschakelt eigen verplichtingen heeft op grond van de AVG.

1.6 Verwerkers die u inschakelt hebben ook eigen verplichtingen zoals het aangaan van een verwerkersovereenkomst met u, het bijhouden van een register van verwerkingen, zorgen voor adequate beveiliging, vragen om toestemming wanneer een onderaannemer (sub-verwerker) wordt ingeschakeld en het melden van datalekken aan u als verwerkingsverantwoordelijke. Wanneer de verwerker die u inschakelt zich primair richt op het verwerken van bijzondere persoonsgegevens (zoals gezondheidsgegevens) dan moet deze bovendien een eigen Functionaris voor de Gegevensbescherming (FG, zie hierna) aanstellen.[8]

2 Wat zijn uw privacy verplichtingen onder de AVG?

2.1 Ten aanzien van iedere gegevensverwerking moet u toetsen of deze voldoet aan de privacy verplichtingen. Het is daarom van belang om alle verwerkingsactiviteiten vooraf in kaart te brengen. Verwerkingsactiviteiten waarmee u als zorgaanbieder te maken kunt krijgen zijn bijvoorbeeld het verwerken van persoonsgegevens van cliënten in een cliëntendossier, het verstrekken van persoonsgegevens aan instanties zoals de gemeente of zorgaanbieders waar u mee samenwerkt en het bijhouden van uw personeelsadministratie. Daarnaast worden ook bij het monitoren van uw werknemers of het aanbieden van Wifi aan uw bezoekers en/of cliënten persoonsgegevens verwerkt. Denk hierbij aan het verwerken van IP of MAC adressen om internet gebruik bij te houden of het meten - ook dit zijn persoonsgegevens die kunnen worden verwerkt door een zorgaanbieder, en ook hiervoor gelden de verplichtingen zoals toegelicht in deze Factsheet AVG.

2.2 Als verwerkingsverantwoordelijke moet u de persoonsgegevens verwerken op rechtmatige en behoorlijke wijze. U moet ervoor zorgen dat de persoonsgegevens die u verwerkt juist en nauwkeurig zijn en dat deze tijdig worden geactualiseerd. Voordat u persoonsgegevens verwerkt, moet u onderzoeken of het doel wat u wil bereiken ook op minder ingrijpende manier kan worden bereikt. Er mogen niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk.[9] Hieronder volgen een aantal meer specifieke verplichtingen uit de AVG met een korte toelichting. Voor zover het gaat om een verplichting die niet reeds onder de Wbp gold, hebben wij dit aangegeven.

---

8 In de Wbp hadden de verwerkers nog geen eigen verplichtingen. In de AVG zijn deze opgenomen in artikelen 28, 30, 32 en 33 AVG. Het aanstellen van de FG vloeit voort uit artikel 37 AVG.

9 De beginselen voor zorgvuldige gegevensverwerking volgen uit internationale en Europese wetgeving, waaronder de OESO Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). De beginselen zijn daarnaast vastgelegd in Art. 6 Wbp en Art. 5 lid 1 AVG. Dit vormt het vertrekpunt voor een rechtmatige gegevensverwerking.

2.2.1 Doelbinding. U mag alleen persoonsgegevens verwerken voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Persoonsgegevens mogen niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze oorspronkelijk zijn verkregen.[10] De doeleinden dienen voorafgaand aan de gegevensverwerking te zijn bepaald en beschreven. In het kader van de uitvoering van de Wmo 2015, de Jeugdwet en de Wlz kan als doeleinde voor het verwerken van persoonsgegevens bijvoorbeeld worden genoemd het bieden/uitvoeren van een algemene voorziening of maatwerkvoorziening, het verlenen van jeugdhulp en het bieden van adequate (langdurige) zorg.

2.2.2 Wettelijke grondslag. In de AVG staan zes grondslagen opgesomd, die gelijk zijn aan de grondslagen uit de Wbp.[11] Persoonsgegevens mogen alleen worden verwerkt als één van die zes grondslagen aanwezig is. De grondslagen komen kort samengevat op het volgende neer:

a) ondubbelzinnige toestemming van de betrokkene;

b) verwerking is noodzakelijk om een overeenkomst te sluiten met de betrokkene of om deze uit te voeren;

c) verwerking is noodzakelijk zodat u kan voldoen aan een wettelijke verplichting;

d) verwerking is noodzakelijk om vitale belangen te beschermen van de betrokkene;

e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang, zoals een publiekrechtelijke taak;

f) u heeft een gerechtvaardigd belang voor de verwerking dat prevaleert ten aanzien van het privacybelang van de betrokkene.

Welke grondslag van toepassing is, is afhankelijk van de wijze waarop persoonsgegevens worden verwerkt en de doeleinden waarvoor dit gebeurt.

Een grondslag kan bijvoorbeeld zijn de toestemming van de betrokkene. Nieuw in de AVG is dat (uitdrukkelijke) toestemming verder is uitgewerkt. Toestemming moet een vrije keuze zijn en moet geïnformeerd, specifiek en ondubbelzinnig worden gegeven. Voorts moet toestemming worden geregistreerd en moet te allen tijde kunnen worden ingetrokken door de betrokkene.[12] Wanneer toestemming voor het verwerken van

10 Art. 7 en 9 Wbp; Art. 5 lid 1 sub b AVG.

11 Art. 8 Wbp; Art. 6 AVG.

12 Art. 8 sub a Wbp; Art. 6 lid 1 sub a AVG. Zie voor verdere invulling van het begrip toestemming artikel 7 AVG, met overweging 32.

persoonsgegevens is 'verstopt' in algemene voorwaarden, wordt dit niet gezien als ondubbelzinnig en specifiek. Deze vorm van toestemming gegeven is daarom niet rechtsgeldig.

Voor wat betreft het vastleggen van cliënt gegevens in een dossier en verstrekking daarvan aan de gemeente cq andere relevante instantie, geldt dat de grondslag kan worden gevonden in een (expliciete) wettelijke verplichting (Wmo 2015, Jeugdwet, Wlz). Hierbij zal steeds nauwkeurig moeten worden onderzocht welke gegevens volgens de specifieke wet moeten worden opgenomen in een dossier en welke gegevens moeten worden verstrekt aan welke instanties.

Ten aanzien van het verwerken van persoonsgegevens van werknemers kan de grondslag bijvoorbeeld worden gevonden in de uitvoering van de arbeidsovereenkomst die u heeft met de werknemer, of in de aanwezigheid van een gerechtvaardigd belang dat u heeft, dat prevaleert ten aanzien van de privacy van de werknemer. Dit laatste kan het geval zijn wanneer u uw systemen logt en monitort zodat u kunt zien wie er toegang heeft gehad tot welke dossiers. Hierbij worden persoonsgegevens van een werknemer verwerkt (bijvoorbeeld een IP adres of personeels-nummer) en heeft u in veel gevallen een gerechtvaardigd bedrijfsbelang. Let op dat toestemming van de werknemer in de meeste gevallen geen rechtsgeldige grondslag zal zijn, omdat deze toestemming niet geheel vrij kan worden gegeven. De werknemer heeft immers een afhankelijkheidsrelatie met een werkgever.

2.2.3 Gezondheidsgegevens. Omdat gezondheidsgegevens bijzondere persoons-gegevens zijn, gelden voor het verwerken daarvan strenge regels. Deze gegevens mogen worden verwerkt door zorgaanbieders, maar dan moet daarbij wel kunnen worden aangetoond dat dit noodzakelijk is met het oog op goede ondersteuning of verzorging van de cliënt, dan wel het beheer van de betreffende instelling.[13]

Gezondheidsgegevens mogen verder alleen worden verwerkt door personen die tot geheimhouding verplicht zijn uit hoofde van hun ambt, beroep of een wettelijk voorschrift dan wel krachtens een overeenkomst. Ook overige personen moeten de persoonsgegevens geheim houden, tenzij de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat hij de gegevens aan andere hiertoe bevoegde personen meedeelt.[14] Dit laatste kan bijvoorbeeld het geval zijn bij een melding aan het advies- en meldpunt huiselijk geweld en kindermishandeling (**AMHK**).

Als niet aan voormelde voorwaarden wordt voldaan, moet voorafgaand aan de verwerking van de gezondheidsgegevens altijd de uitdrukkelijke, geïnformeerde toestemming van uw cliënt worden gevraagd, hetgeen u als

[13] Art. 16 en 21 Wbp; Art. 9 lid 1, 2 sub h en 3 AVG en Uitvoeringswet AVG (nog niet aangenomen).

[14] Art. 21 Wbp; Art. 9 lid 2 sub h en 3 AVG en Uitvoeringswet AVG (nog niet aangenomen).

verwerkingsverantwoordelijke moet kunnen aantonen. U moet ook toestemming vragen als een bijzondere wet zoals de Wmo 2015, de Jeugdwet of de Wlz voorschrijft dat voorafgaande toestemming verplicht is.

2.2.4 BSN. Hoewel volgens de AVG een BSN geen bijzonder persoonsgegeven is zoals een gegeven dat iets zegt over de gezondheid, gelden voor het verwerken van het BSN toch specifieke regels vanwege de gevoelige aard hiervan en het risico op (identiteits)fraude. Het verwerken van het BSN mag alleen als dit door een specifieke wet wordt voorgeschreven.[15]

Als zorgaanbieder zult u ook het BSN van uw cliënten moeten verwerken, omdat u aan de hand van dat nummer uw cliënt moet kunnen identificeren. Dit gebeurt bijvoorbeeld in de Wmo 2015, de Jeugdwet en de Wlz. In de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg staat dat zorgaanbieders het BSN van hun cliënt kunnen gebruiken om de zorg te kunnen verlenen. De zorgaanbieder is verplicht het BSN vast te leggen in de administratie. In de Wet cliëntenrechten elektronische gegevens is voorts bepaald dat bij elektronische gegevensuitwisseling tussen zorgaanbieders eveneens het BSN kan worden uitgewisseld, voor zover dit noodzakelijk is voor het doel van de uitwisseling.

2.2.5 Documentatieplicht. Waar op grond van de Wbp gegevensverwerkingen in beginsel moeten worden gemeld bij de Autoriteit Persoonsgegevens (**AP**) of de Functionaris voor de Gegevensbescherming,[16] geldt vanaf de inwerkingtreding van de AVG de documentatieplicht.[17] Deze documentatie-plicht houdt in dat u in een (intern) register alle gegevensverwerkingen bijhoudt die u uitvoert. U hoeft de gegevensverwerking dan niet meer te melden aan de AP.

In uw register van verwerkingsactiviteiten moet u in ieder geval vastleggen voor welke doeleinden u persoonsgegevens verwerkt, op welke categorieën van betrokkenen de persoonsgegevens betrekking hebben, aan wie de persoonsgegevens kunnen worden versterkt, welke bewaartermijnen gelden en welke beveiligingsmaatregelen u hebt genomen.[18]

2.2.6 Informatieplicht. U bent als verwerkingsverantwoordelijke verplicht om de betrokkenen, zoals uw cliënten, bezoekers en uw werknemers, te informeren over de gegevensverwerkingen die u uitvoert. U moet deze betrokkenen onder andere informeren over wie u bent en voor welke doeleinden u de persoonsgegevens verwerkt. De AVG schrijft daarboven

15 In de Wbp werd het BSN niet gekwalificeerd als 'bijzonder persoonsgegeven' maar werd de gevoelige aard daarvan onderkend in art. 24 Wbp. Art. 4 lid 15 en Art. 87 AVG en Uitvoeringswet AVG (nog niet aangenomen).

16 Art. 24 Wbp, zie voor de bepaling over de Functionaris voor de Gegevensbescherming onder de Wbp art. 62 Wbp.

17 Art. 30 AVG.

18 Art. 30 AVG.

ook voor dat u moet aangeven wat de grondslag is voor de gegevensverwerking, met wie de persoonsgegevens worden gedeeld, hoe lang de persoonsgegevens worden bewaard, wie de Functionaris voor de Gegevensbescherming is en dat betrokkenen bij klachten contact op kunnen nemen met de AP.[19]

De informatie aan de betrokkenen kan bijvoorbeeld worden opgenomen in een privacy statement dat wordt verstrekt *voorafgaand* aan de gegevensverwerking. Denk hierbij ook aan een hoofdstuk over persoonsgegevens in uw personeelshandboek, een flyer aan uw cliënten, informatie die wordt getoond wanneer uw cliënten of de bezoekers gebruik gaan maken van uw Wifi netwerk. De wijze waarop u de informatie verstrekt is afhankelijk van de gegevensverwerking zelf en wie de betrokkenen zijn.

2.2.7 Bewaartermijn. U mag de persoonsgegevens niet langer bewaren dan noodzakelijk voor de doeleinden waarvoor u de persoonsgegevens heeft verzameld.[20] Er staan geen vaste bewaartermijnen in de Wbp en in de AVG. Deze bewaartermijnen kunnen wel voortvloeien uit specifieke wetgeving. Dit gebeurt bijvoorbeeld in de Wet op de Geneeskundige Behandelingsovereenkomst (**WBGO**), waarin een algemene maximum bewaartermijn wordt voorgeschreven van 15 jaar.[21] Deze termijn geldt voor alle verwerkingen die samenhangen met de WGBO, waaronder ook verwerkingen kunnen vallen met betrekking tot de uitvoering van de Wlz (die geen eigen bewaartermijn kent). In de Wmo 2015 en de Jeugdwet is eveneens een minimale bewaartermijn van 15 jaar voorgeschreven ten aanzien van cliëntgegevens.

2.2.8 Overeenkomsten sluiten met derden. Wanneer u met een derde samenwerkt en wanneer er binnen deze samenwerking persoonsgegevens worden verwerkt (bijvoorbeeld doordat deze worden uitgewisseld of toegankelijk worden gemaakt), moet u vaststellen wat de privacyrechtelijke rol is van uzelf en van deze derde: is er sprake van een verwerkingsverantwoordelijke die een verwerker inschakelt of van twee verwerkingsverantwoordelijken? Afhankelijk daarvan moet u specifieke schriftelijke privacy afspraken maken. Onderscheid kan hierbij worden gemaakt tussen de volgende twee situaties:

19 Art. 33 en 34 Wbp; Art. 13 en 14 AVG.

20 Art. 10 Wbp; Art. 5 lid 1 sub e AVG.

21 De VGN heeft in 2008 voor haar leden een richtlijn gemaakt over de toepassing van de WGBO in de gehandicaptensector. De richtlijn is op 3 april 2008 aangenomen door de Algemene Ledenvergadering en is op 1 januari 2009 ingegaan. Hierin wordt ook ingegaan op de te hanteren bewaartermijnen. Meer informatie vindt u hier: http://www.vgn.nl/artikel/2171

a) Verwerkersovereenkomst (voorheen Bewerkersovereenkomst).[22] Wanneer u een derde inschakelt die handelt als verwerker namens u, bijvoorbeeld een leverancier van een cliënten dossier, moet u met deze verwerker een verwerkersovereenkomst sluiten.[23] De AVG stelt wettelijk vast welke onderdelen er in de verwerkersovereenkomst moeten worden opgenomen. Zo eist de AVG bijvoorbeeld dat de verwerkersovereenkomst afspraken bevat over de instructieplicht, beveiliging, de meldplicht datalekken en het inzetten van onderaannemers als sub-verwerker.[24]

b) Verantwoordelijke - verantwoordelijke overeenkomst. Ook tussen twee partijen die ieder als verwerkingsverantwoordelijke kwalificeren moeten op grond van de AVG afspraken worden gemaakt. Dit is bijvoorbeeld het geval wanneer verschillende zorgaanbieders samenwerken en/of samen zorgconcepten ontwikkelen en in het kader van deze samenwerking persoonsgegevens uitwisselen. De AVG schrijft voor dat deze afspraken onder andere moeten gaan over de wijze waarop betrokkenen hun rechten kunnen uitoefenen en de wijze waarop de betrokkenen over de gegevensverwerking worden geïnformeerd.

2.2.9 Beveiligingsmaatregelen. De verwerkingsverantwoordelijke moet ervoor zorgen dat de gegevensverwerking adequaat wordt beveiligd en moet passende organisatorische en technische beveiligingsmaatregelen nemen die ervoor zorgen dat persoonsgegevens niet verloren gaan of onrechtmatig worden verwerkt.[25] Wat passend is, is afhankelijk van de gebruikelijke technieken en de gevoeligheid van de persoonsgegevens. De Wbp noemt geen voorbeelden van beveiligingsmaatregelen, maar de AVG noemt onder andere pseudonimisering en versleuteling, systemen om integriteit en beschikbaarheid te garanderen en procedures om de genomen maatregelen periodiek te testen.[26]

2.2.10 Meldplicht datalekken: Een datalek is een inbreuk op de beveiliging van persoonsgegevens die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde toegang of verstrekking van de verwerkte persoonsgegevens. Een datalek moet binnen 72 uur worden gemeld aan de AP als er een risico bestaat voor de rechten en

---

22 Op het moment van publicatie van deze Factsheet AVG is de VGN in samenwerking met de andere leden van de Brancheorganisaties Zorg een model verwerkersovereenkomst aan het ontwikkelen voor haar leden. In de nog te publiceren verwerkersovereenkomst zullen deze eisen uit de AVG terug komen. In het najaar (2017) zal de verwerkersovereenkomst gereed zijn.

23 Art. 14 Wbp en de Richtsnoeren Beveiliging Persoonsgegevens (2013) van de AP; Art. 28 lid AVG.

24 Op het moment van publicatie van deze Factsheet AVG is de VGN in samenwerking met de andere leden van de Brancheorganisaties Zorg een model verwerkersovereenkomst aan het ontwikkelen voor haar leden. In de nog te publiceren verwerkersovereenkomst zullen deze eisen uit de AVG terug komen. In het najaar (2017) zal de verwerkersovereenkomst gereed zijn.

25 Art. 13 Wbp en de Richtsnoeren Beveiliging Persoonsgegevens (2013) van de AP; Art. 32 AVG.

26 Art. 32 AVG.

vrijheden van de betrokkenen. Dit kan bijvoorbeeld worden aangenomen wanneer bijzondere persoonsgegevens zijn gelekt. Wanneer er sprake is van een hoog privacy risico, bijvoorbeeld wanneer deze bijzondere persoonsgegevens niet versleuteld waren, moet dit ook worden gemeld aan de betrokkenen.[27]

2.2.11 Functionaris voor de gegevensbescherming (**FG**). Als zorgaanbieder bent u op grond van de AVG vanaf 25 mei 2018 verplicht om een FG aan te stellen. De Wbp kende ook al een FG maar het aanstellen daarvan was niet verplicht.[28] Deze verplichting uit de AVG gaat mogelijk voor u al eerder gelden, omdat het aanstellen van een FG ook wordt voorgeschreven in het 'Besluit elektronische gegevensverwerking door zorgaanbieders'.[29] Dit besluit is op het moment dat deze Factsheet AVG is opgesteld nog niet aangenomen.

De nieuwe verplichting om een FG aan te stellen gaat voor u gelden omdat u op grote schaal gezondheidsgegevens verwerkt. De AVG bevat specifieke eisen waaraan de FG moet voldoen. De Artikel 29 Werkgroep, een samenwerkingsverband van Europese privacy toezichthouders, heeft in april 2017 de (definitieve) Guidelines on Data Protection Officers gepubliceerd (thans alleen in het Engels, zie hier) die meer uitleg geven over het aanstellen van een FG, de eisen die aan de FG worden gesteld en wat zijn taken zijn.

Een FG moet worden aangesteld op basis van zijn of haar professionele kwaliteiten en inhoudelijke expertise van het recht en de praktijk. De FG moet onafhankelijk zijn of haar taken kunnen uitvoeren en rechtstreeks rapporteren aan het management. De FG kan iemand zijn die binnen de organisatie ook andere taken uitvoert, zolang geen sprake is van een belangenconflict. Dit is bijvoorbeeld het geval wanneer de FG ook een positie binnen het management bekleedt en beslist over bepaalde gegevensverwerkingen, zoals een bestuurder of hoofd van de HR afdeling.[30]

De FG hoeft niet noodzakelijkerwijs iemand uit uw eigen organisatie te zijn, het is denkbaar dat een externe FG wordt aangesteld. Deze FG kan voor verschillende organisaties (al dan niet zorgaanbieders) werkzaam zijn voor zover dit niet tot belangenconflicten leidt.

---

27 Art. 34a Wbp en de Beleidsregels meldplicht datalekken (2015) van de AP, Art. 4 lid 12, 33 en 34 AVG AVG.

28 Art. 62 Wbp, Art. 37 AVG.

29 Art. 2 Besluit elektronische gegevensverwerking door zorgaanbieders. Het gaat hierbij om instellingen als bedoeld in artikel 1, eerste lid, van de Wet kwaliteit klachten en geschillen zorg die zijn aangesloten op een elektronisch uitwisselingssysteem.

30 Art. 37 en 38 AVG.

2.2.12 Data Privacy Impact Assessment (**DPIA**). Een gegevenseffectbeoordeling of DPIA is een instrument om vooraf de privacy-risico's van een gegevensverwerking in kaart te brengen. De DPIA stimuleert u om op tijd na te denken over de impact die een project heeft op de privacy van betrokkenen, op welke wijze de persoonsgegevens compliant kunnen worden verwerkt en of er ook een aanpak mogelijk is die minder gevolgen heeft voor de privacy van betrokkenen.

De DPIA is op grond van de AVG verplicht als u verwacht dat een bepaalde gegevensverwerking een hoog privacy-risico oplevert voor de betrokkenen.[31] Dit kan bijvoorbeeld het geval zijn wanneer bij een verwerkingsactiviteit veel bijzondere persoonsgegevens (zoals gezondheidsgegevens) worden verwerkt zoals bij cliënt registratie systemen. Bij de invoering van een nieuw systeem zal dan een DPIA moeten worden uitgevoerd.

2.2.13 Rechten van betrokkenen. Betrokkenen hebben op grond van de Wbp al bepaalde privacy rechten. Patiënten, werknemers, bezoekers of anderen van wie persoonsgegevens verwerkt worden hebben bijvoorbeeld het inzage- en correctierecht, het recht op persoonsgegevens te laten verwijderen en zich tegen verwerking te verzetten. De AVG heeft de rechten van betrokkenen uitgebreid en onder andere toegevoegd dat een betrokkene kan verzoeken de gegevensverwerking te beperken of zijn gegevens door te laten geven aan een nieuwe aanbieder (data portabiliteit).[32]

2.2.14 Doorgifte. Persoonsgegevens mogen alleen worden doorgegeven binnen de Europese Economische Ruimte (EER) of naar landen buiten de Europese Economische Ruimte (EER) die volgens de Europese Commissie een passend beschermingsniveau bieden. Een overzicht van deze landen vindt u hier. Daarbuiten is doorgifte alleen toegestaan indien bepaalde formaliteiten zijn vervuld.[33]

31 Art. 35 lid 3 AVG.

32 Art. 35, 36, 40 en 41 Wbp; Art. 14 -21 AVG

33 Hoofdstuk 11 Wbp; Hoofdstuk V AVG

3 Toezicht en handhaving

3.1 De AP houdt toezicht op de naleving van de privacy regelgeving. Deze toezichthouder kan een last onder dwangsom opleggen indien de privacy regelgeving niet wordt nageleefd. Op grond van de Wbp kunnen boetes oplopen tot EUR 820.000 of tot 10% van de jaaromzet van een organisatie.

3.2 Onder de AVG wordt de boetebevoegdheid van de AP uitgebreid. Na 25 mei 2018 kan de AP boetes opleggen die kunnen oplopen tot het maximum van EUR 20 miljoen of 4% van de omzet van een onderneming, als dit hoger is. Naast deze boetes blijft de AP bevoegd om een last onder dwangsom op te leggen, of bestuursdwang toe te passen. Ook blijft de mogelijkheid bestaan dat betrokkenen een verwerkingsverantwoordelijke kunnen aanspreken en in rechte betrekken en kunnen zij klagen bij de Ombudsman. Wanneer publiek bekend wordt dat een zorgaanbieder op inbreukmakende wijze met persoonsgegevens omgaat, bijvoorbeeld doordat een onderzoek van de AP openbaar wordt gemaakt of door een betrokkene die ruchtbaarheid hieraan geeft, kan dit leiden tot reputatieschade.[34]

[34] Hoofdstuk 9 Wbp; Hoofdstuk VII AVG

STAPPENPLAN

4 Welke acties zijn noodzakelijk om AVG compliant te worden?

Om ervoor te zorgen dat u klaar bent voor de AVG moet u tijdig een aantal acties nemen. Voordat u hiermee aan de slag gaat, is het aan te raden om te inventariseren waar uw organisatie nu staat: in hoeverre voldoet uw organisatie al aan de geldende privacy verplichtingen? Welke acties heeft u al ondernomen? Wanneer u weet waar u nu staat, kunt u onderstaande drie fasen doorlopen met bijbehorende actiepunten.

Naast het doorlopen van onderstaande acties raden wij aan om binnen de organisatie duidelijk te communiceren dat u werkt naar meer privacy compliance en raden wij aan het privacy bewustzijn in alle schakeringen van uw organisatie te vergroten door bijvoorbeeld trainingen aan te bieden of een informatiebijeenkomst te organiseren.

Fase 1: De fundering: aanwijzen van bevoegde personen en vastleggen van gegevens-verwerkingen

- Bepaal wie binnen uw organisatie verantwoordelijk zal/zullen zijn voor het AVG compliance project.
- Stel tijdig vast wie de FG is.
- Breng in kaart welke gegevensverwerkingen er binnen uw organisatie plaatsvinden zodat kan worden voldaan aan de documentatieverplichting. Het is raadzaam om hiervoor gebruik te maken van een IT-tool, die door verschillende (commerciële) partijen op de markt worden gebracht. Hou er rekening mee dat binnen uw organisatie niet alleen gegevens worden verwerkt van uw cliënten, maar ook van uw werknemers en relaties.
- Valideer de gegevensverwerkingen die in kaart zijn gebracht.
- Controleer welke derde partijen betrokken zijn bij de gegevensverwerkingen. Zijn er verwerkers en mede-verwerkingsverantwoordelijken?
- Check de afspraken die zijn gemaakt met de verwerkers en medeverwerkings-verantwoordelijken.
- Documenteer alle datalekken die hebben plaatsgevonden / plaatsvinden, ook wanneer u meent dat deze datalekken niet hoeven te worden gemeld aan de AP en/of de betrokkenen. Geef aan waarom u meent dat wel of niet melding aan de AP en/of de betrokkenen noodzakelijk was/is.

Fase 2: De uitvoering: Implementatie van de AVG

- Zorg ervoor dat alle relevante documentatie is verzameld. Denk daarbij aan de afspraken met derden die persoonsgegevens verwerken (verwerkers en medeverwerkings-verantwoordelijken), relevante documentatie over de wijze waarop werknemers met persoonsgegevens omgaan, privacy policies, toestemmingsformulieren en bewaarbeleid.

- Sluit of actualiseer verwerkersovereenkomsten. Check welke standaard verwerkers-overeenkomsten uit de branche kunnen worden gebruikt.[35]

- Sluit overeenkomsten met mede-verwerkingsverantwoordelijken.

- Controleer de beveiligingsmaatregelen en verbeter deze waar nodig. Let op dat niet alleen technische beveiligingsmaatregelen worden genomen waarbij bestanden worden beveiligd en versleuteld. Denk bij het nemen van beveiligingsmaatregelen ook aan organisatorische beveiligingsmaatregelen zoals het trainen van werknemers met betrekking tot het omgaan met vertrouwelijke informatie en persoonsgegevens. Check welke werknemers noodzakelijkerwijs toegang moeten hebben tot welke (onderdelen van) gegevensbestanden en log deze toegang.

- Actualiseer het beveiligingsbeleid.

- Actualiseer privacy statements en interne privacy beleidsdocumenten.

- Actualiseer het bewaarbeleid.

- Stel vast in welke gevallen de toestemming vereist is en update toestemmingsformulieren.

- Maak een zogenoemde 'roadmap voor datalekken'. Dit is een document of schema dat inzicht geeft in de maatregelen die moeten worden genomen om datalekken te voorkomen en daarop te reageren. In dergelijk document staat hoe u als zorgaanbieder voorkomt dat datalekken plaatsvinden en hoe uw organisatie reageert op datalekken. Ook komt hierin te staan wat er gebeurt nadat een datalek heeft plaatsgevonden en hoe maatregelen die zijn genomen naar aanleiding van een datalek worden geëvalueerd. De roadmap datalekken bevat ook een instructie ten aanzien van de wijze waarop datalekken intern moeten worden gedocumenteerd.

- Maak aanpassingen in uw systemen die mogelijk maken dat betrokkenen hun rechten uitoefenen, waaronder hun inzagerecht en het recht om vergeten te worden.

- Wanneer uw zorgaanbieder een Ondernemingsraad heeft, moet voor het aanpassen van het beleid met betrekking tot het verwerken van persoonsgegevens om instemming worden gevraagd.

[35] Op het moment van publicatie van deze Factsheet AVG is de VGN in samenwerking met de andere leden van de Brancheorganisaties Zorg een model verwerkersovereenkomst aan het ontwikkelen voor haar leden. In de nog te publiceren verwerkersovereenkomst zullen deze eisen uit de AVG terug komen. In het najaar (2017) zal de verwerkersovereenkomst gereed zijn.

Fase 3 - De controle. Check de voortdurende processen en stuur bij waar nodig

- Actualiseer de documentatie van de gegevensverwerkingen. Pas indien nodig de gegevensverwerkingen aan of voeg nieuwe gegevensverwerkingen toe.

- Controleer op regelmatige basis de beveiligingsmaatregelen. Wanneer een derde beveiligingsmaatregelen namens u heeft genomen, zorg ervoor dat u regelmatig een audit uitvoert / laat uitvoeren, bijvoorbeeld eenmaal per jaar. Controleer wie er toegang hebben (gehad) tot de gegevens door middel van logging.

- Controleer of uw roadmap datalekken wordt gevolgd, en of deze aanpassing behoeft. Controleer of datalekken daadwerkelijk zijn gedocumenteerd en op de juiste wijze.

- Wanneer nieuwe gegevensverwerkingen worden verwacht, waarvoor een DPIA is vereist, start tijdig met het voorbereiden en uitvoeren van de DPIA.

- Controleer regelmatig, bijvoorbeeld jaarlijks, de overeenkomsten die u heeft met derden (mede-verwerkingsverantwoordelijken en verwerkers), check of de overeenkomsten worden nageleefd en controleer of bijsturing noodzakelijk is. Maak gebruik van het audit recht dat u heeft op grond van de overeenkomst.

- Controleer of beleidsdocumenten ten aanzien van het omgaan met persoonsgegevens worden nageleefd. Check regelmatig of het privacy statement nog actueel is en afdoende informatie over de gegevensverwerkingen omvat.

Deze Factsheet informeert zorgaanbieders over hun belangrijkste privacy verplichtingen in het kader van de AVG. Deze Factsheet geeft een algemeen overzicht en ziet niet op specifieke gegevensverwerkingen. Wij hebben bovendien bij het opstellen van deze Factsheet niet gestreefd naar volledigheid.

Naast de AVG is ook andere wetgeving op u van toepassing waarin specifieke privacy verplichtingen staan, zoals de Wmo 2015, de Jeugdwet en de Wlz. Wij wijzen daarnaast onder meer op de WGBO en de Wet BIG. Deze Factsheet dient niet ter vervanging van juridisch advies. Bij twijfel over de stappen die u moet nemen bij een concrete gegevensverwerking raden wij u aan zo nodig nader juridisch advies in te winnen.

De Factsheet: 'Omgaan met persoonsgegevens door zorgaanbieders: Algemene Verordening Gegevensbescherming (AVG)' is een uitgave van de Vereniging Gehandicaptenzorg Nederland (VGN) en is tot stand gekomen in samenwerking met Van Doorne N.V.

Oudlaan 4
3515 GA Utrecht

Postbus 413
3500 AK Utrecht

T 030-27 39 300
F 030-27 39 387

www.vgn.nl
info@vgn.nl