Algemene verordening gegevensbescherming
betekenis voor de zorgsector

1. Inleiding

Het op geautomatiseerde wijze verwerken van gegevens is misschien wel de belangrijkste 'industrie' van onze samenleving. Big data is here to stay. Redenen waarom de Europese wetgever het beschermen van de privacy van haar burgers naar een hoger niveau tilt. Op 25 mei 2018 treedt de zogenaamde Algemene verordening gegevensbescherming (AVG) in werking. Ook de zorgsector krijgt hiermee te maken.

De AVG komt in de plaats van de Wet bescherming persoonsgegevens (Wbp) en zorgt voor een stevige verbetering van de privacyrechten van burgers. De AVG creëert voor overheden, bedrijven en zorginstellingen nieuwe verplichtingen. Anders dan de Wbp kent de AVG forse boetes bij niet-naleving.[1]

Uit onderzoek blijkt dat privacy binnen de meeste zorginstellingen de laatste jaren meer aandacht heeft gekregen, maar dat er nog veel te verbeteren valt.[2] Naar aanleiding hiervan heeft het ministerie van VWS het 'Aktieplan (informatie)beveiliging patiëntgegevens' opgesteld.

Hieronder volgt een overzicht van de belangrijkste veranderingen die de AVG meebrengt voor zorginstellingen.

2. Toestemming als verwerkingsgrondslag

Net als onder de werking van de Wbp blijkt het verkrijgen van toestemming van de persoon aan wie de gegevens toebehoren als de belangrijkste rechtsgrondslag om zijn gegevens te mogen verwerken.[3] Anders dan de Wbp stelt de AVG strenger eisen aan het gebruik maken van

1. Dit artikel behandelt niet de boetes die de AVG introduceert en de rechtsbescherming hiertegen. Zie voor een samenvatting hiervan 'De Algemene verordening gegevensbescherming: een introductie voor de zorgsector', mr. C. van Balen en mr. O.S. Nijveld, Tijdschrift voor Gezondheidsrecht 2017/8, blz. 619 e.v.
2. Beveiliging van patiëntgegevens, adviesbureau PBLQ, Kamerstukken II 2017/17, 31765, 259. Zie ook 'De Algemene verordening gegevensbescherming: een introductie voor de zorgsector', mr. C. van Balen en mr. O.S. Nijveld, Tijdschrift voor Gezondheidsrecht 2017/8, blz. 607 e.v.
3. Toestemming is niet altijd vereist om gegevensverwerking te legitimeren. Gegevensverwerking kan ook worden gebaseerd op een noodzaak. Zie 'Handleiding Algemene verordening gegevensbescherming', Ministerie van Justitie en Veiligheid, januari 2018, blz. 34 e.v.

toestemming als grondslag voor gegevensverwerking:

a) de toestemming moet vrij zijn gegeven. Dit betekent dat iemand daadwerkelijk de vrije keuze moet hebben om te weigeren, zonder dat hieraan nadelige gevolgen zijn verbonden. Als er sprake is van een afhankelijkheidsrelatie dan zal niet snel sprake kunnen zijn dat toestemming vrij is gegeven. Dit betekent dat in zo'n geval de gegevensverwerking niet gebaseerd kan zijn op toestemming;[4]
b) als een verwerking meerdere doeleinden heeft, moet voor elk afzonderlijk doel toestemming worden verleend;
c) toestemming mag nooit impliciet worden gegeven; er moet altijd sprake zijn van een duidelijke actieve handeling (duidelijke 'akkoord' of het aanvinken van een vakje op een website). Opting out (het uitvinken van een als default aangevinkt vakje) is geen toestemming. Toestemming moet ondubbelzinnig zijn. Op de verwerkingsverantwoordelijke rust de bewijslast om aan te tonen dat toestemming op een geldige wijze is verleend;
d) de betrokkene mag te allen tijde zijn toestemming intrekken. Vóór het verlenen van toestemming moet de betrokkene hierover zijn geïnformeerd. Het intrekken van toestemming moet net zo gemakkelijk zijn als het verlenen ervan (bijvoorbeeld het 'uitvinken' van het vakje op een website). Het intrekken van toestemming heeft geen terugwerkende kracht;
e) het verzoek om toestemming en het aangeven voor welke doeleinden de toestemming wordt verleend moet duidelijk en beknopt zijn. De AVG maakt een einde aan het verstoppen van informatie over het verwerken van persoonsgegevens in lange teksten.

Wanneer een organisatie vóór de inwerkingtreding van de AVG persoonsgegevens verwerkt met toestemming van betrokkenen, dan moet zij nagaan of de wijze waarop die toestemming is verkregen in overeenstemming is met de nieuwe eisen die de AVG stelt. Is dat het geval dan hoeft de organisatie niet opnieuw om toestemming te vragen. Is dit niet het geval dan dient de organisatie opnieuw toestemming te vragen!

3. Nieuwe rechten betrokkenen

De AVG kent nieuwe rechten toe aan betrokkenen. Hieronder een korte omschrijving van deze nieuwe rechten.

3.1 Het verwijderingsrecht of 'the right to be forgotten'

Onder de huidige Wbp hebben betrokkenen het recht om een organisatie te vragen om onjuiste, onvolledige of niet meer ter zake doende persoonsgegevens te verwijderen. De AVG breidt dit verwijderingsrecht uit. Als de betrokkene zich beroept op het verwijderingsrecht moeten zijn persoonsgegevens worden verwijderd op het moment dat een in de verordening genoemde situatie zich voordoet:

1. de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;

4. Wanneer de uitvoering van een overeenkomst afhankelijk is van het geven van toestemming voor een andere verwerking die niet noodzakelijk is voor de uitvoering van de overeenkomst ('bundelen'), dan rijst de vraag of toestemming vrijelijk gegeven kan worden. Zie 'Handleiding Algemene verordening gegevensbescherming', idem, blz 38.

2. de betrokkene trekt zijn toestemming voor het verwerken in en dit is de enige grondslag waarop de verwerking berust of kan berusten;
3. de betrokkene heeft gegrond bezwaar gemaakt tegen de verwerking;
4. de persoonsgegevens zijn onrechtmatig verwerkt;
5. de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op de organisatie rust;
6. de persoonsgegevens zijn verzameld in verband met een rechtstreeks aanbod van internetdiensten aan een kind.

Naast het recht om zijn gegevens te verwijderen heeft de betrokkene het recht 'om vergeten te worden' (the right to be forgotten). Het betreft situaties waarbij een organisatie persoonsgegevens van de betrokkene openbaar heeft gemaakt, bijvoorbeeld door deze gegevens online te zetten. In dat geval dient de organisatie naast het verwijderen van de gegevens uit de eigen systemen redelijke technische en organisatorische maatregelen te nemen om andere organisaties die de persoonsgegevens verwerken ervan op de hoogte te stellen dat de betrokkene 'vergeten wil worden'. Dat houdt in dat elke koppeling naar, kopie of reproductie van de gegevens gewist moeten worden.[5]

Het verwijderingsrecht of het recht om vergeten te worden gelden niet onverkort. Onder bepaalde omstandigheden is een organisatie niet verplicht om gegevens te wissen. Deze uitzondering kan voor sommige zorginstellingen van belang zijn. Bijvoorbeeld indien gegevens nodig zijn om redenen van algemeen belang op het gebied van volksgezondheid, wetenschappelijk of statistisch onderzoek.[6]

3.2 Recht op dataportabiliteit

De betrokkene heeft onder de werking van de AVG het recht op dataportabiliteit (overdraagbaarheid van gegevens). Dit houdt in om een kopie van de persoonsgegevens die aan een verwerkingsverantwoordelijke zijn verstrekt in een gestructureerde, gangbare en machineleesbare vorm te ontvangen, en deze persoonsgegevens ongehinderd over te dragen aan een andere verwerkingsverantwoordelijke. Het doel van het recht dataportabiliteit is de zeggenschap van de betrokkene over zijn gegevens te vergroten. In beginsel mag de organisatie geen kosten in rekening brengen voor de uitoefening van dit recht. Het recht van dataportabiliteit mag geen afbreuk doen aan het recht van anderen, daaronder begrepen het (medisch) beroepsgeheim.[7]

Het recht op dataportabiliteit ziet uitsluitend op digitale gegevens. Papieren dossiers vallen er niet onder. Het recht ziet alleen op gegevens die met toestemming van de betrokkene zijn verwerkt. Dit is van belang voor zorginstellingen aangezien zorgverlening in de regel plaats vindt op grond van toestemming van de cliënt (informed consent) en ter uitvoering van een geneeskundige behandelingsovereenkomst. Van belang is dat het medische dossier in de zin van artikel 7:454 BW niet zonder meer gelijk staat met de verwerking van persoonsgegevens zoals bedoeld in de Wbp en

5. Zie 'Handleiding Algemene verordening gegevensbescherming', blzz. 78 - 79.
6. Artikel 17, lid 3, AVG.
7. Zie 'De Algemene verordening gegevensbescherming: een introductie voor de zorgsector', mr. C. van Balen en mr. O.S. Nijveld, Tijdschrift voor Gezondheidsrecht 2017/8, blz. 614.

de AVG.[8] Niet onder het medische dossier vallen persoonlijke aantekeningen van de medische hulpverlener, waardoor deze aantekeningen ook niet onder het recht op dataportabiliteit vallen.

4. Verplichtingen voor organisaties

Centraal staat in de AVG dat organisaties de verplichting hebben om aan te tonen hoe zij de AVG naleven. Dit betekent dat organisaties moeten kunnen aantonen dat zij voldoen aan eisen omtrent rechtmatigheid van de verwerking, transparantie naar de betrokkene, doelbinding en juistheid. Hiernaast moeten organisaties kunnen aantonen dat zij verantwoorde technische en organisatorische maatregelen hebben genomen om persoonsgegevens te beschermen.[9] De AVG schrijft niet precies voor hoe de verwerkingsverantwoordelijke dit aantoont. Wél schrijft de AVG bepaalde instrumenten voor om de verwerking van persoonsgegevens te verantwoorden:

1. het register van verwerkingsactiviteiten;
2. het uitvoeren van een gegevensbeschermingseffectbeoordeling (data privacy impact assessment; DPIA);
3. het bijhouden van een register van datalekken die binnen de organisatie zijn opgetreden;
4. het aantonen van gegeven toestemmingen indien de verwerking op basis van toestemming plaatsvindt.

Register van verwerkingsactiviteiten
Het register van verwerkingsactiviteiten geldt niet voor een organisatie met minder dat 250 werknemers. Deze uitzondering geldt niet indien de organisatie bijzondere persoonsgegevens verwerkt. Dit betekent dat zorginstellingen met minder dan 250 werknemers tóch gehouden zijn om een register bij te houden aangezien zij in de regel bijzondere persoonsgegevens van patiënten verwerken.

Gegevensbeschermingseffectbeoordeling
Het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) moet resulteren in:[10]

a) een beschrijving van de beoogde verwerking en de doelen voor die verwerking;
b) een oordeel over de noodzakelijkheid en evenredigheid van de verwerking met het oog op het vastgestelde doel;
c) een oordeel over de risico's voor betrokkenen;
d) de beoogde maatregelen in de zin van waarborgen, veiligheidsmaatregelen en mechanismen om die risico's weg te nemen of te beperken.

Het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) is niet onder alle omstandigheden verplicht. Een DPIA is wél verplicht voor verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van de betrokkenen. Hiervan is onder meer sprake bij het systematisch op geautomatiseerde wijze verwerken van aspecten van persoonsgegevens (profiling), het systematisch monitoren van openbare ruimten en grootschalige verwerking van

8. Zie 'Asser serie 7 IV, Bijzondere overeenkomsten, opdracht, incl. de geneeskundige behandelingsovereenkomst en de reisovereenkomst', bewerkt door mr. T.F.E. Tjong Tjin Tai, Kluwer, 2009, nr. 427.
9. Artikel 24, lid 1 AVG.
10. Zie 'Handleiding Algemene verordening gegevensbescherming', blz. 59.

bijzondere persoonsgegevens.[11] Voor een zorginstelling is dus van belang te onderkennen wanneer sprake is van de waarschijnlijkheid van een hoog risico en grootschalige verwerking.

Een ambtelijke werkgroep van Europese privacy toezichthouders heeft criteria ontworpen om aan te geven wanneer sprake is van hoog risico en grootschalige verwerking.[12] Naar aanleiding hiervan kan voorzichtigheidshalve worden geconcludeerd dat sprake is van een risico wanneer:

a) gevoelige gegevens of gegevens met een hoog persoonlijk karakter worden verwerkt
b) en gegevens die betrekking hebben op kwetsbare betrokkenen (denk aan ouderen, wilsonbekwamen, kinderen en patiënten).[13]

Voor wat betreft het begrip grootschalige verwerking stelt de ambtelijke werkgroep dat verwerkingen van bijzondere persoonsgegevens door individuele artsen niet als grootschalige verwerkingen worden aangemerkt; waardoor een DPIA niet verplicht is. Het verwerken van bijzondere gegevens door een ziekenhuis is dat wél. Alles er tussen in is onduidelijk.

Uit het bovenstaande valt op te maken dat een zorginstelling eerder wél DPIA-plichtig zal zijn dan niet.

5. Conclusie en aanbevelingen

De AVG is vanaf 25 mei 2018 van toepassing. De AVG introduceert nieuwe privacy rechten en verplichtingen en werkt rechtstreeks, zonder de noodzaak van transformatie naar nationale wetgeving. Betrokkenen krijgen nieuwe rechten: het recht 'om vergeten te worden' en het recht op dataportabiliteit. De AVG legt veel meer dan de huidige Wbp de nadruk op aantoonbaarheid. Anders dan onder de Wbp moeten organisaties zich veel meer inspannen om aan te tonen hoe zij voldoen aan de AVG voldoen.

Uit onderzoek blijkt dat zorginstellingen nog een behoorlijke stap moeten zetten om te kunnen voldoen aan de AVG. Het verdient aanbeveling om deze stap niet zomaar als een privacy project te zien. Het door zorginstellingen integer en veilig omgaan met gegevens van hun patiënten of cliënten vormt een wezenlijk deel hun maatschappelijke doelstelling en professionaliteit. Het verbeteren van privacy kan beter organisatiebreed worden ingezet als onderdeel van de cultuur die de zorginstelling naleeft. Patiënten en cliënten centraal stellen kan niet zonder hun privacy aantoonbaar te waarborgen.

Geadviseerd wordt om het implementeren van de AVG niet als een losse privacy project op te pakken. Borg de AVG binnen de organisatie vanuit het centraal stellen van de patiënt en cliënt. Hierdoor ontstaat ook verbinding met de (komende veranderingen op hun terrein van) cliëntmedezeggenschap binnen de zorg en het serieus nemen van klachten en geschillen. Een AVG project die hierop aansluit heeft niet alleen meer kans van slagen, maar zal door medewerkers niet worden ervaren als een 'moetje', maar als een bijdrage aan het centraal stellen van de belangen en behoeften van patiënten en cliënten.

11. Artikel 35 AVG.
12. Groep gegevensbescherming artikel 29
13. Zie 'De Algemene verordening gegevensbescherming: een introductie voor de zorgsector', mr. C. van Balen en mr. O.S. Nijveld, Tijdschrift voor Gezondheidsrecht 2017/8, blz. 617.

ZorgopKoers B.V.
mr. H.F.L. Goverde
web: www.zorgopkoers.nl
e-mail: henry.goverde@zorgopkoers.nl
telefoon: 06 5315 3456