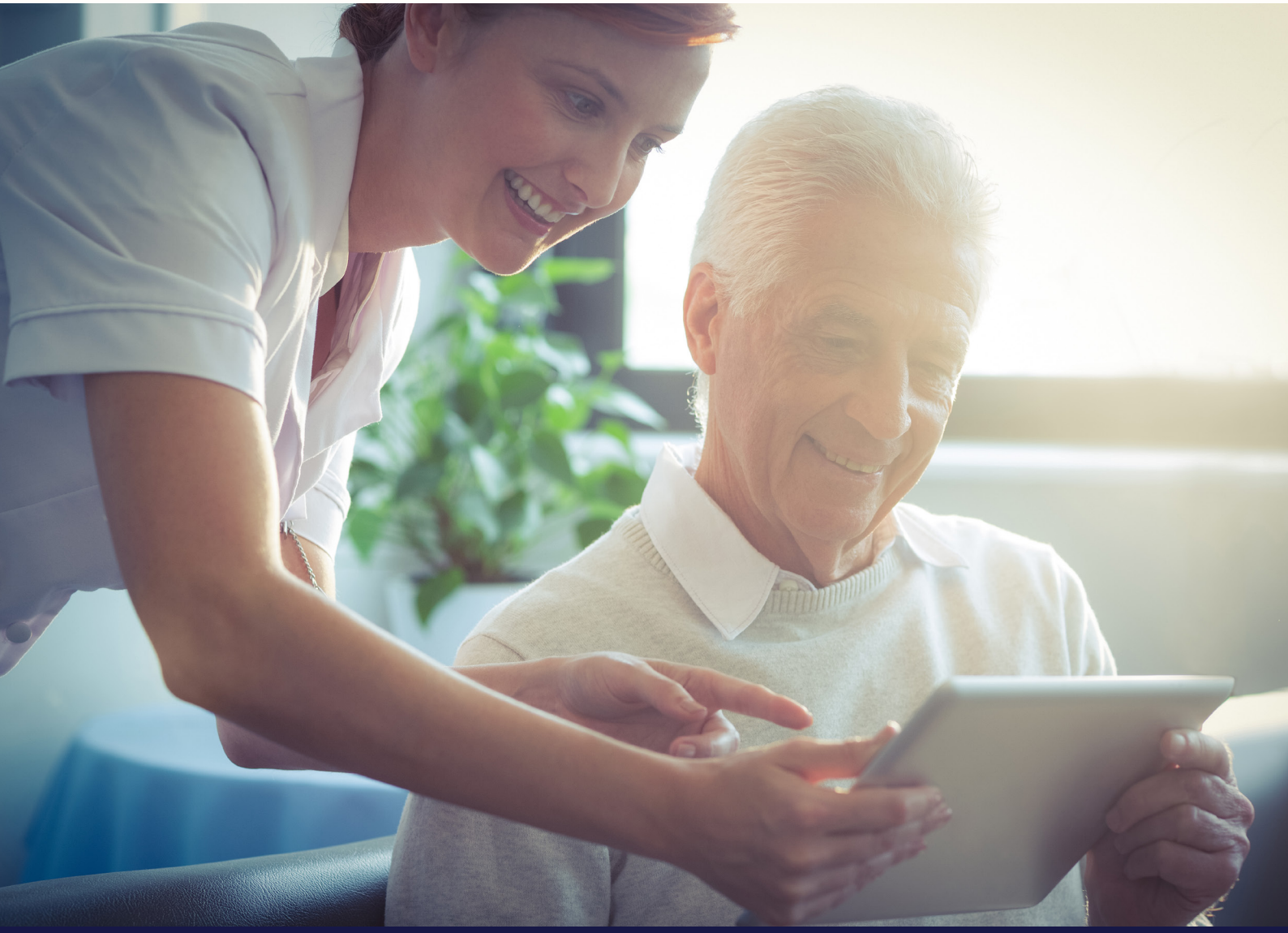
BMC
YACHT GROUP

Proactief omgaan met gegevens van cliënten; de DPIA in de praktijk



Partners in verbetering

Met de komst van de AVG per 25 mei 2018 zijn er een paar dingen veranderd in de omgang met persoonsgegevens in de zorg. Maar niet alles is nieuw: de belangrijkste uitgangspunten zijn hetzelfde gebleven. Grondslag, doelbinding, het verbod op het verwerken van bijzondere persoonsgegevens en beveiliging zijn onderwerpen die ook vóór 25 mei 2018 van toepassing waren.

Wel nieuw is onder andere dat je een register van verwerkingen moet hebben, dat je aantoonbaar de AVG moet naleven en dat je in sommige situaties een Data Protection Impact Assessment (DPIA) moet uitvoeren. De DPIA is bedoeld om vooraf risico's van een bepaalde gegevensverwerking te kunnen inschatten en tijdig passende maatregelen te nemen om die risico's te beperken.

DPIA meer dan een administratielast

De praktijk leert dat het uitvoeren van een DPIA niet alleen een verplichting is, maar de organisatie ook daadwerkelijk helpt om scherp te krijgen wat het doel van de verwerking is, welke gegevens daarvoor noodzakelijk zijn en op welke wijze dat binnen de kaders van de AVG kan worden gerealiseerd. In veel gevallen is het niet de vraag of een verwerking mag, maar wel op welke manier en binnen welke randvoorwaarden dat kan, bijvoorbeeld door alleen strikt noodzakelijke gegevens te gebruiken en door een strikt autorisatieschema voor toegang toe te passen. De uitkomsten van een DPIA kunnen ook in een aanbesteding worden gebruikt. Hiermee kan aan een aanbieder helder worden aangegeven aan welke eisen een product of dienst moet voldoen. Daarmee wordt voorkomen dat er een standaardproduct wordt aangeboden waarin de benodigde faciliteiten ontbreken.

Op grond van artikel 35 AVG is een DPIA in een aantal gevallen verplicht. Of een DPIA verplicht is kan worden beoordeeld op basis van artikel 35 lid 1 AVG (algemeen), artikel 35 lid 3 (specifiek) of

[1] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

artikel 35 lid 4 (de lijst van de AP). Ook kan gebruikgemaakt worden van de opinie 248 van de WP29. En ook heeft de Autoriteit Persoonsgegevens een lijst gepubliceerd van verwerkingen waarvoor een DPIA verplicht is. Tevens verwacht de toezichthouder dat ook voor bestaande verwerkingen eenmaal in de drie jaar een DPIA uit wordt gevoerd. De gedachte daarbij is dat het uitvoeren van een DPIA geen eenmalige opdracht is, maar een continu proces.

Bezint eer gij begint

Als uw organisatie concludeert dat een DPIA verplicht is, moet deze DPIA voorafgaand aan de verwerking worden uitgevoerd. Op de website van de toezichthouder is te lezen dat je niet met de gegevensverwerking mag beginnen voordat de DPIA en indien nodig een voorafgaande raadpleging is uitgevoerd. [1] Je mag dus niet alvast beginnen.

Het toch beginnen met de verwerking zonder DPIA waar deze wel verplicht is brengt risico's met zich mee. De Functionaris voor de Gegevensbescherming (FG) zal in zijn toezichthoudende rol niet anders kunnen concluderen dan dat dit een overtreding van de AVG is. In zijn gesprekken met het bestuur en in zijn jaarverslag is dit een onderwerp en mogelijk ook in de publiciteit, nog los van het feit dat ook de toezichthouder met uitgebreide bevoegdheden en sanctiemogelijkheden dit niet door de vingers kan zien.

Kijken naar de toekomst: inventarisatie DPIA's

Verstandiger is dus om bij wijziging van een bestaande verwerking of bij een nieuwe verwerking van persoonsgegevens waarvoor een DPIA verplicht is voorafgaand een DPIA uit te voeren. Maar hoe zorg je dat je hiervoor voldoende tijd hebt en dat je voorbereid bent? Dat kan door jaarlijks een inschatting te maken van het aantal verwachte DPIA's en hiervan een lijst samen te stellen. Hoe maak je die lijst?

Hierbij kan het register van verwerkingen behulpzaam zijn. Op basis van dit register kan beoordeeld worden welke verwerkingen bij veranderingen in aanmerking komen voor een DPIA, gelet op de AVG, de WP29 opinie 248 en de lijst van de Autoriteit Persoonsgegevens. Daarnaast kan worden gekeken naar gegevensverwerkingen die langer dan drie jaar geleden zijn aangevangen.

> "In veel gevallen is het niet de vraag of een verwerking mag, maar wel op welke wijze deze binnen de kaders van de wet kan worden uitgevoerd"

Op basis van deze selectie kan worden bekeken voor welke van de verwerkingen in de komende jaren wijzigingen op stapel staan. Wijzigingen bijvoorbeeld als gevolg van investeringen in nieuwe systemen, veranderende wetgeving of voorgenomen veranderingen in samenwerkingen of werkwijzen. Zo kan een een planning worden gemaakt voor het uitvoeren van DPIA's. Daarmee is voorzienbaar of een DPIA verplicht is en kan deze tijdig worden uitgevoerd.

Complexiteit bepalend voor benodigde tijd en geld

Daarnaast kan worden beoordeeld of er vermoedelijk sprake zal zijn van een complexe DPIA of van een meer eenvoudige. Dit is niet alleen relevant omdat het betekenis heeft voor het kennisniveau van degene die de DPIA uitvoert, maar ook in ver-

band met de tijdsinvestering en de doorlooptijd. Over het algemeen zullen gegevensverwerkingen in het sociaal- en zorgdomein complexer zijn, gelet op de complexere materie, het beroepsgeheim,de wetgeving, de aard van de gegevens en de hoeveelheid keten- of netwerkpartners die erbij betrokken is. Een meer intern gericht proces, zoals een onderdeel van de financiële administratie, kan mogelijk eenvoudiger te beoordelen zijn.

Proactief omgaan met gegevens van cliënten

Belangrijk is dus ook om indien nodig tijdig budget te reserveren voor het uitvoeren van DPIA's waarvoor intern geen capaciteit is of waarvoor het aan expertise ontbreekt. Regeren is vooruitzien en met het vooraf inschatten van de benodigde DPIA's wordt niet alleen aan een wettelijke verplichting voldaan, maar wordt vooral bijgedragen aan een verantwoorde gegevensverwerking die de uitvoering van de zorgtaak optimaal ondersteunt.

Meer weten over DPIA's of de uitvoering ervan?

Neem dan contact op met een van onze senior adviseurs Julius Duijts, Alex Commandeur of Willem de Vries. Zij kunnen u helpen bij de vragen die u heeft over DPIA's. Bijvoorbeeld of een DPIA verplicht is en wat de complexiteit ervan is. Daarnaast kunnen onze adviseurs ondersteunen bij de uitvoering van DPIA's. Indien gewenst bespreken zij graag de mogelijkheden daarvoor. Ook voor andere vragen over de implementatie van de AVG staan ze u graag te woord.

Ir. Julius Duijts CISSP CIPP/E
senior adviseur
06 - 29 52 55 31
julius.duijts@bmc.nl

mr. Alex Commandeur
senior adviseur
06 - 82 12 03 17
alex.commandeur@bmc.nl

drs. Willem de Vries
senior adviseur
06 - 51 62 97 80
willem.de.vries@bmc.nl

Kijk voor meer informatie ook eens op onze website **www.bmc.nl**