

5 krachtige tips voor het omgaan met patiëntgegevens en AVG

DPIA in het algemeen

Als organisaties persoonsgegevens (laten) verwerken, moeten ze onderzoeken of die verwerking tot risico's leidt voor patiënten of cliënten, en of er manieren zijn om die risico's weg te nemen. Zo'n onderzoek heet een gegevensbeschermingseffectbeoordeling, in het Engels: een *Data Protection Impact Assessment*, oftewel DPIA.

Soms is een DPIA verplicht en soms ook niet. Ook als het niet verplicht is, kan het nuttig zijn. Bekijk dit [overzicht](#) van wanneer een DPIA verplicht is.

DPIA in de zorg

Een DPIA richt zich op de privacyrisico's voor de patiënt/cliënt en dus niet de risico's die de zorginstelling loopt. De zorginstelling loopt ook risico's zoals boetes en reputatieschade.

In de DPIA gaat het er om wat er kan gebeuren als de gegevens van de patiënt/cliënt verkeerd worden gebruikt. Dus de mogelijke gevolgen voor de patiënt/cliënt. Omdat in de zorg veel medische gegevens worden verwerkt, kunnen de gevolgen groot zijn.

Een DPIA helpt om na te denken hoe groot deze risico's zijn en of de risico's kleiner kunnen worden gemaakt. Bijvoorbeeld door gegevens anoniem te maken of heel kort te bewaren.

De zorg is een sector waarvoor extra regels uit wet- en regelgeving gelden. Denk bijvoorbeeld aan het medisch beroepsgeheim. De gevoeligheid van de gegevens brengt ook met zich mee dat extra aandacht nodig is als leveranciers worden ingezet die de gegevens buiten de Europese Unie verwerken.

Voer de DPIA uit voordat je besluit de gegevens te verwerken

Je kunt een DPIA zien als hulpmiddel voor het nemen van een besluit om gegevens te verwerken. Start daarom de DPIA zo vroeg mogelijk. Als het kan al bij het maken van de plannen of het project waarin jouw zorginstelling gegevens gaat verwerken.



Gebruik de DPIA-aanbeveling in **Privacy Nexus**

Zo kun je bepalen voor welke bestaande verwerkingen het aanbevolen is om een DPIA uit te voeren. En verbindt de DPIA vervolgens aan de specifieke verwerking zodat je **aan kunt tonen** dat je een DPIA hebt uitgevoerd voor al je verwerkingen met een hoog risico.

Gebruik een **gestandaardiseerde vragenlijst** voor het uitvoeren van de DPIA's

Op deze manier kun je tijd besparen en een zekere kwaliteit van de informatie garanderen. Het format in Privacy Nexus gebruikt **gesloten vragen** waar mogelijk, beperkt het gebruik van juridische terminologie en **'neemt je bij hand'** gedurende het proces.

Vraag de Functionaris Gegevensbescherming (FG) om advies

Als jouw organisatie een FG heeft moet hij/zij adviseren over de DPIA. Zorg er ook voor dat dit advies wordt gedocumenteerd. In Privacy Nexus kun je als FG gebruik maken van de **FG-beoordeling functionaliteit** waarmee je de DPIA kunt beoordelen en deze kunt goedkeuren of afwijzen.

Maak gebruik van **bestaande** **informatie**

Veel andere organisaties in de zorg zullen **vergelijkbare verwerkingsactiviteiten** doen. De verwerkingen van het ene GGD/GGZ/verzorghuis zullen waarschijnlijk niet veel afwijken van het andere. Kijk wat er beschikbaar is aan openbare informatie. Branche-organisaties zoals NFU, NVZ en de Nederlandse ggz bieden mogelijk **templates** of voor de branche uitgevoerde DPIA's aan.

Zie bijvoorbeeld het [adviesdocument](#) van de zorg- en veiligheidshuizen. Templates zijn ook beschikbaar in Privacy Nexus. Overweeg tenslotte om jouw DPIA's ook te delen of te publiceren. Zo help je anderen.

Met eigen ogen zien hoe Privacy Nexus
jouw organisatie kan ondersteunen bij
de privacy-administratie? Neem contact
met ons op voor een demo of vrijblijvend
testaccount.

contact@privacynexus.io
+31(0)70 8209690

KANTOOR NEDERLAND
Maanweg 174
2516 AB den Haag

KANTOOR DUITSLAND
Friedrichstrasse 68
10117 Berlijn



5 krachtige tips
voor het omgaan met
patiëntgegevens en AVG