De GDPR in 10 stappen

Stap 9- DPO en DPIA

De GDPR in 10 Stappen

Stap 9 – DPO en DPIA

Inleiding

Deze termen zullen u misschien niet direct bekend in de oren klinken. DPO is de Engelse afkorting voor 'functionaris voor gegevensbescherming'. DPIA is de Engelse afkorting voor 'gegevensbeschermingseffectbeoordeling'. Twee al even moeilijke woorden, reden te meer om ze in een afzonderlijke stap wat beter te duiden.

Functionaris voor gegevensbescherming (DPO)

Een functionaris voor gegevensbescherming is iemand die als onafhankelijke partij mee waakt over uw privacybeleid.

De GDPR bepaalt dat u zo'n functionaris moet aanstellen wanneer u :

- Hoofdzakelijk belast bent met verwerkingen die vanwege hun aard, omvang en/of doeleinden een regelmatige en stelselmatige observatie op grote schaal vereist van de betrokkenen;
- Hoofdzakelijk belast bent met grootschalige verwerking van bijzondere categorieën van persoonsgegevens (zie de definitie in stap 2) en van strafrechtelijke gegevens.

Voor zorgverstrekkers is de tweede categorie relevant. Zij verwerken immers per definitie 'bijzondere categorieën van persoonsgegevens', namelijk gezondheidsgegevens.
De vraag of een zorgverstrekker een DPO moet aanstellen, hangt dan ook af van de vraag of de verwerking van die gevoelige gegevens moet beschouwd worden als een 'grootschalige verwerking'.
Helaas geeft de GDPR ook hier geen verdere verduidelijking van wat als ' grootschalige verwerking' moet worden gezien. Wel zegt de GDPR heel uitdrukkelijk dat een ziekenhuis daar wél onder valt (en dus een DPO moet aanstellen), terwijl een individuele zorgverstrekker daar niet onder valt (en dus géén DPO moet aanstellen).

<u>Wat met de tussencategorieën, zoals groepspraktijken?</u>

Noch de GDPR, noch de Belgische of Europese Toezichthouder geeft een antwoord op die vraag. Dat wil dus zeggen dat elke groepspraktijk in principe zelf moet nagaan of er sprake kan zijn van 'grootschalige verwerking'.

Groepspraktijken worden in de praktijk op verschillende manieren ingedeeld. Binnen de zogenaamde monodisciplinaire praktijken is er sprake van kleine dan wel grote groepspraktijken naargelang er tot 5 dan wel meer zorgverleners samenwerken.
Het groepsverband kan feitelijk zijn, waarmee wordt bedoeld dat de zorgverleners onder één dak gevestigd zijn, dan wel virtueel, waarbij er sprake is van een formele samenwerking, maar zonder gemeenschappelijk (praktijk)gebouw. In deze beide vormen van praktijk wordt de patiëntenpopulatie over het algemeen als één geheel beheerd met een gemeenschappelijk dossiersysteem. Dit wordt zo opgevat dat een zorgverlener toegang heeft of kan hebben tot de dossiers van alle patiënten. Dat is net één van de redenen waarom er in een groepspraktijk wordt samengewerkt.
Daartegenover staat een zogenaamd permanentienetwerk waarbij enkel afspraken worden gemaakt over vervangingen.

Essentieel is dan ook de beoordeling of er sprake is van een “zakelijk” dan wel een “professioneel” team. Zakelijk is de samenwerking waarbij de nadruk ligt op het realiseren van gemeenschappelijke voorwaarden en voorzieningen zoals afspraken rond wachtdienst, vervangingen of faciliteiten. Aan de andere kant is er het “professionele” team met een eigen identiteit waarbij de nadruk ligt op het gemeenschappelijk leveren van goede zorg met een hoge graad aan medisch-inhoudelijk overleg en duidelijke afspraken over het te voeren beleid.

Vuistregel kan zijn dat waar er geen gemeenschappelijk medisch beleid en er eerder sprake is van ‘solopraktijken onder één dak’, er geen noodzaak is om formeel een DPO aan te stellen.
Bij zogenaamde multidisciplinaire praktijken die ook nog eerstelijnspraktijken worden genoemd, zal het meer voorkomen dat er gegevens over patiënten tussen de zorgverleners worden gedeeld. In dat geval kan men de verwerker wellicht al sneller grootschalig noemen.

In Nederland heeft de Nederlandse toezichthouder wel een specifieke regeling uitgewerkt voor groepspraktijken van huisartsen en ‘andere specialistische zorg dan ziekenhuizen’. De Nederlandse toezichthouder gaat er daarbij van uit dat een dergelijke groepspraktijk aan grootschalige verwerking doet wanneer ze

- ✓ meer dan 10.000 ingeschreven patiënten heeft of gemiddeld meer dan 10.000 patiënten per jaar behandelt, én
- ✓ de gegevens van deze patiënten in één informatiedossier bewaren

Dit zijn richtlijnen van de Nederlandse toezichthouder, die dus geen juridische waarde hebben in België. Maar omdat de GDPR in eerste instantie niet zozeer kijkt naar de beslissingen die u in het kader van de GDPR neemt, maar wel naar de *verantwoording* en *argumentatie* van die beslissing, kan de Nederlandse richtlijn mogelijks ook hier in België een leidraad vormen, althans voor de groepspraktijken van huisartsen en ‘ andere specialistische zorgverstrekkers’[1].

Zolang de Belgische toezichthouder zelf geen richtlijn heeft uitgevaardigd, doet u er best aan om in geval van twijfel, toch een DPO aan te stellen.

[1] Deze term ‘andere specialistische zorgverstrekkers wordt verder niet gedefinieerd. Uit de beslissing lijkt men wel te kunnen afleiden dat bijvoorbeeld apothekers er niet onder vallen.

Gegevensbeschermingseffectbeoordeling (DPIA)

De GDPR bepaalt dat u voordat u een verwerking start, een beoordeling moet uitvoeren van het effect van die verwerking op de rechten en vrijheden van de betrokkenen. Maar dat moet alleen wanneer de verwerking een hoog risico inhoudt voor die rechten en vrijheden. Dit kan bijvoorbeeld het geval zijn bij:

- ✓ Het toekennen van een evaluatie of een score (inclusief profiling en voorspelling), in het bijzonder wanneer ze gebaseerd zijn op persoonlijke aspecten van de betrokkene zoals zijn werkprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, gedrag, loyaliteit, of verplaatsingen;
- ✓ Geautomatiseerde besluitvorming met een juridisch of vergelijkbaar gevolg (bijvoorbeeld: automatische verwerking van gegevens die beslissen om iemand wel of niet als klant, leverancier, … toe te laten)
- ✓ Stelselmatige monitoring van natuurlijke personen (bijvoorbeeld op publiek toegankelijke ruimten)
- ✓ De niet -occasionele verwerking van gevoelige gegevens of de verwerking van gegevens van zeer persoonlijke aard
- ✓ Gegevens die op grote schaal worden verwerkt
- ✓ Matching of samenvoeging van datasets
- ✓ Gegevens over kwetsbare personen (kinderen, geesteszieken, bejaarden, …)
- ✓ Het gebruik van nieuwe technologieën (of nieuwe toepassingen van bestaande technologieën), waarvan de impact op de risico's voor persoonsgegevens nog niet is onderzocht.
- ✓ Verwerking van gegevens die de toegang tot een bepaalde dienst kan verhinderen (bijvoorbeeld een bank die haar klanten screent op grond van kredietinformatie om te bepalen of ze al dan niet een lening toekent.

De GDPR bepaalt ook hier uitdrukkelijk:
"De verwerking van persoonsgegevens mag niet als een grootschalige verwerking worden beschouwd als het gaat om de verwerking van persoonsgegevens van patiënten of cliënten door een individuele arts, een andere zorgprofessional of door een advocaat. In die gevallen mag een gegevensbeschermingseffectbeoordeling niet verplicht worden gesteld."

Individuele zorgverleners moeten met andere woorden geen DPIA uitvoeren. Dat wordt ook bevestigd door de Belgische toezichthouder.

Voor groepspraktijken ligt de situatie, net zoals bij de vraag of een DPO moet worden aangesteld, anders. Als vuistregel geldt dat u best een beoordeling opstelt van zodra 2 van deze 9 criteria vervuld zijn. Aangezien zorgverleners in een groepspraktijk in de meeste gevallen zullen voldoen aan minsten twee van de 9 criteria ('grootschalige verwerking' en ' gegevens over kwetsbare personen'), en het bovendien gaat om een kernactiviteit, zal een DPIA in de regel nodig zijn.

De bedoeling van zo'n beoordeling is vooraf na te gaan wat de impact ervan is of kan zijn op de rechten van de betrokkenen. Daarbij kan gebruik worden gemaakt van al bestaande studies, mits deze voldoende worden geconcretiseerd naar de situatie in België.

Zo'n beoordeling bevat ten minste:

- ✓ Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder in voorkomend geval de gerechtvaardigde belangen die u inroept;
- ✓ Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- ✓ Een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen;
- ✓ De beoogde maatregelen om de risico's aan te pakken.

Wanneer uit deze beoordeling zou blijken dat de verwerking inderdaad een hoog risico zou opleveren indien u geen maatregelen neemt om het risico te beperken, moet u voorafgaand aan de verwerking de Gegevensbeschermingsautoriteit raadplegen.

Checklist

- ❑ Ik weet wat een DPO en een DPIA is, en wanneer ik daar (geen) gebruik van moet maken.
- ❑ Ik heb in mijn Verwerkingsregister omschreven waarom ik er desgevallend geen gebruik van moet maken.