Eldermans | Geerts

DPIA Product

Inleiding

Vrijwel alle zorgaanbieders moeten ingevolge artikel 35 van de AVG vroeg of laat een Data Protection Impact Assesment (DPIA)[1] uitvoeren, omdat gewerkt wordt met bijzondere persoonsgegevens. Een DPIA is een risicoanalyse voorafgaand aan een nieuwe verwerking van persoonsgegevens. Daarmee worden de gevonden risico's beperkt. Zo heeft de organisatie de verwerkingen beter in kaart. Daarmee is de DPIA een hulpmiddel bij besluitvorming.

Het is goed om te weten hoe een DPIA werkt en daarmee aan de slag te gaan, zodat u kunt aantonen u bewust te zijn van uw verplichtingen, zowel richting toezichthouders als uw cliënten. Het is niet ingewikkeld, maar wel nodig. Dit product geeft u handvatten om snel en gemakkelijk de wettelijk vereiste beoordeling te doen.

Inhoudsopgave

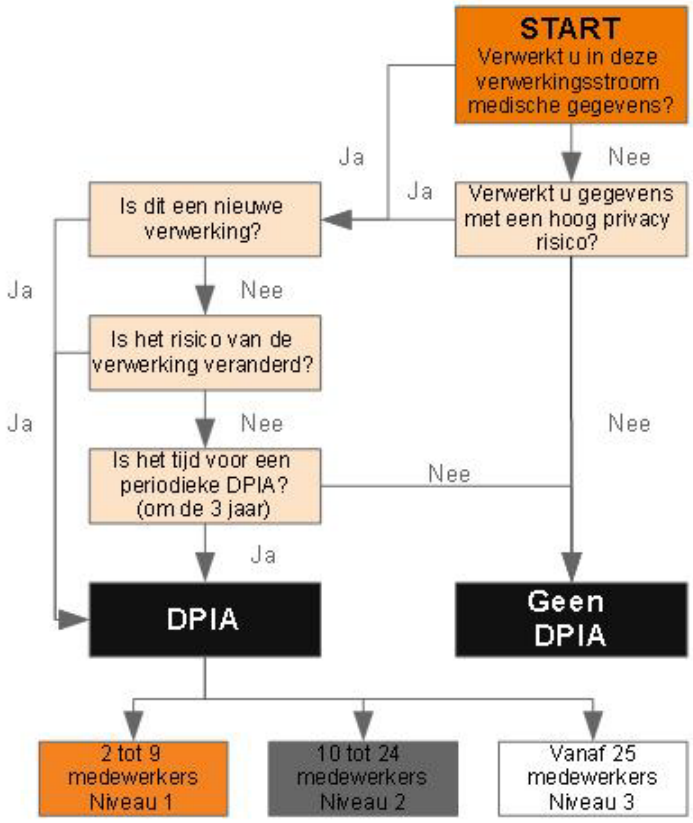
Verplichting DPIA 2
Niveau DPIA 2
Stap 1: Team formeren 2
Stap 2: Informatie verzamelen 3
Stap 3: Stakeholders consulteren 4
Stap 4: In kaart brengen risico's 4
Stap 5: Risico's beoordelen 5
Stap 6: Maatregelen nemen 6
Stap 7: Rapport opstellen 8
Stap 8: Evaluatie 8
Bijlage 1: Team 10
Bijlage 2: Documenten 11
Bijlage 3: Vragenlijst 12
Bijlage 4: Leeg rapport 13

[1] Een DPIA wordt ook wel PIA of gegevensbeschermingseffectbeoordeling genoemd.

Verplichting DPIA

Via het schema kunt u nagaan of u een DPIA moet doen. Neem voor het doorlopen van het schema een concrete (nieuwe) verwerking in gedachten, bijvoorbeeld de verwerkingen in de salarisadministratie. U kunt de verwerkingsstromen uit het verwerkingsregister als uitgangspunt gebruiken. Toets dit elk jaar.

- Het is niet verplicht om elke 3 jaar een DPIA te doen. De AP adviseert dit wel.
- Het schema geeft een advies over het niveau van de DPIA.[2]
- Binnen een eenmanszaak zonder personeel is geen DPIA verplicht.



Niveau DPIA

De wet geeft niet aan hoe een DPIA precies vormgegeven moet worden. Het is logisch dat een ziekenhuis een meer omvattender DPIA moet doen dan een kleine praktijk. Daarom onderscheiden we 3 niveaus. Zodat elke zorgaanbieder een DPIA kan doen die past bij het formaat van de organisatie.

Niveau 1: Simpel	2 tot 9 medewerkers
Niveau 2: Laag	10 tot 24 medewerkers
Niveau 3: Midden	Vanaf 25 medewerkers

Voor grote partijen kan het aan te raden zijn een meer omvangrijke DPIA te doen. Voor maatwerk kunt u contact met ons opnemen via post@eldermans-geerts.nl.

[2] Een verwerking met een hoog privacy risico is onder meer: *heimelijk onderzoek, zwarte lijsten, fraudebestrijding, creditscores, financiële situatie, gezondheidsgegevens, samenwerkingsverbanden, (flexibel) cameratoezicht, controle werknemers, locatiegegevens, communicatiegegevens, internet of things, profiling, observatie en beïnvloeding gedrag.*

Stap 1: Team formeren

Besloten moet worden wie de DPIA zal doen. Het mooiste is een team met verschillende expertises. Gegevensbescherming heeft zowel een juridisch als technisch element. Indien een FG aanwezig is, moet deze betrokken worden en adviseren over de DPIA. Het is verstandig de DPIA te laten uitvoeren door een ander dan de verantwoordelijke voor de nieuwe verwerking. Desgewenst kan ook een verwerker betrokken worden. Zie bijlage 1 voor een overzicht van mensen die in het team opgenomen kunnen worden.

Een teamlid
Twee teamleden ☐ FG, indien niet aanwezig zorgaanbieder ☐ ICT
Drie teamleden ☐ FG/jurist ☐ Zorgaanbieder ☐ ICT

Stap 2: Informatie verzamelen

Voordat gestart wordt met de DPIA moet duidelijk zijn om welke informatie het gaat. Het verwerkingsregister kan als uitgangspunt gebruikt worden. Alle bestaande verwerkingsstromen staan in het verwerkingsregister. Bij een nieuwe verwerking moet grofweg dezelfde informatie als in het verwerkingsregister bekend zijn. In het rapport moet de verwerking beschreven worden.

☐ Maak het verwerkingsregister volledig. ☐ Beschrijf de verwerking waar de DPIA op ziet in het rapport (context), beschrijf: soort persoonsgegevens, type persoonsgegevens (bijzonder of niet?), verwerkingsstromen, betrokken partijen, verwerkingslocatie, betrokkenen, voorgestelde techniek en bewaartermijnen. ☐ Noodzaak en evenredigheid: beoordeel of de verzamelde informatie nodig is voor de verwerking. ☐ Doelbinding: beoordeel of de informatie passend is voor het doel.
Idem
Idem

Stap 3: Stakeholders consulteren

U verwerkt persoonsgegevens van anderen. Van belang is dan ook op de hoogte te zijn van de belangen van de betrokkenen. U kunt onder andere informatie verzamelen met een generieke studie, enquêtes of het betrekken van vertegenwoordigers denk aan een cliëntenraad. Een afwijking van de mening van de betrokkenen moet gedocumenteerd worden.

Bestudeer de belangen van stakeholders of motiveer waarom u dit niet heeft gedaan.	**Stakeholders**: hulpverleners cliënten, medewerkers, mantelzorgers, leveranciers samenwerkingspartners, gemeenten, belangenverenigingen.
Bestudeer de belangen van stakeholders en spreek met één persoon uit de belangrijkste groep stakeholders. In de zorg zal dat vaak de patiënt zijn. Of motiveer waarom u dit niet heeft gedaan.	
Treed in overleg met de drie belangrijkste stakeholders en bestudeer de belangen van de overige stakeholders. Of motiveer waarom u dit niet heeft gedaan.	

Stap 4: In kaart brengen risico's

Het onderzoek naar de risico's kan aanvangen. Het onderzoek wordt gedaan door het doorlopen van een vragenlijst (bijlage 3) en het bekijken van de aanwezige stukken. Welke stukken een rol spelen, kunt u vinden in bijlage 2. Uit het onderzoek moeten de risico's van de verwerking blijken. Denk daarbij aan de beschikbaarheid[3], integriteit[4] en vertrouwelijkheid.[5]

1. U doorloopt de vragenlijst 2. Aanwezigheid stukken
1. Ieder teamlid doorloopt de vragenlijst 2. Beoordeel de uitkomst van de vragenlijst → Tijdens deze bespreking kunnen aanvullingen ontstaan ook buiten de vragenlijst om 3. Aanwezigheid stukken 4. Beoordeel kwaliteit stukken
1. Ieder teamlid doorloopt de vragenlijst

[3] Beschikbaarheid: kunt u de gegevens altijd inzien indien nodig? Zijn er voorzieningen getroffen als aan back-up, de juiste authenticatie en noodstroom.
[4] Integriteit: zijn de gegevens juist en volledig en kunt u dit nagaan/garanderen?
[5] Vertrouwelijkheid: enkel bevoegde personen mogen toegang hebben tot de gegevens.

2. Beoordeel de uitkomst van de vragenlijst
→ Tijdens deze bespreking kunnen aanvullingen ontstaan ook buiten de vragenlijst om
3. Aanwezigheid stukken
4. Beoordeel kwaliteit stukken

Stap 5: Risico's beoordelen

U hebt aan de hand van stap 4 inzage in de risico's (i). Nu is het zaak om de risico's te beoordelen. Enkele vragen zijn hierbij van belang.

i.	Hoe waarschijnlijk is het dat deze gevolgen intreden?	risico's inschatten
ii.	Wat is de ernst als deze gevolgen intreden?	risico's inschatten
iii.	Risico's beoordelen.	risico's beoordelen

De risico's beoordeelt u door ze in te delen in categorieën: laag, matig, hoog, zeer hoog. Deze bepaalt u door de kans (iv) maal de ernst van de gevolgen (v) te doen. Gebruik bij de risico-inschatting de volgende matrixen:

iv. Kans

Zeer klein	Uiterst geringe mogelijkheid van optreden
Klein	Zou kunnen optreden, maar zal in vrijwel alle gevallen niet optreden
Middelmatig	Mogelijk; optreden niet onwaarschijnlijk
Groot	Zeer goed mogelijk; zal in een groot deel van de gevallen optreden
Zeer groot	Zal zeker of vrijwel zeker optreden

v. Ernst gevolgen

Gevolg-klasse	Gevolgen voor patiënten	Gevolgen voor de betrokken organisaties	Gevolgen voor de maatschappij
Laag	□ Geen lichamelijke en/of psychische schade bij patiënten	□ Gering verlies van middelen/ bezittingen □ Geringe financiële gevolgen □ Geen imagoschade	□ Geen maatschappelijke impact
Midden	□ Beperkte lichamelijke en/of psychische schade bij een beperkt aantal patiënten	□ Verlies van middelen/ bezittingen Financiële gevolgen □ Imagoschade	□ Zeer beperkte maatschappelijke impact
Hoog	□ Omvangrijke lichamelijke en/of psychische schade bij een beperkt tot groot aantal patiënten en/of overlijden van één patiënt	□ Aanzienlijk verlies van middelen/ bezittingen □ Aanzienlijke financiële gevolgen □ Omvangrijke imagoschade	□ Beperkte maatschappelijke impact
Zeer Hoog	□ Omvangrijke lichamelijke en/of psychische schade bij een zeer groot aantal patiënten en/of overlijden van meerdere patiënten	□ Faillissement/ sluiting zorginstelling of vergelijkbare gevolgen	□ Omvangrijke maatschappelijke impact

vi. Risico's beoordelen

Kans ▶ Gevolg ▼	Zeer klein	Klein	Middel-matig	Groot	Zeer Groot
Zeer hoog					Zeer hoog risico
Hoog				Hoog risico	
Midden			Matig risico		
Laag		Laag risico			

Per risico moet beoordeeld worden of maatregelen genomen moeten worden. Begonnen moet worden met het afdichten van de hoge risico's. Zowel de hoge als zeer hoge risico's moeten afgedicht worden voordat gestart wordt met de verwerking.

Stap 6: Maatregelen nemen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de risico's te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Motiveer waarom dit restrisico acceptabel is:

- ☐ Geef aan welke hoge privacy risico's uit uw DPIA u niet volledig kunt voorkomen.
- ☐ Vermeld specifiek in welke situatie(s), of met betrekking tot welke onderdelen, er sprake is van een hoog restrisico.
- ☐ Geef aan hoe waarschijnlijk het u lijkt dat de omschreven situatie zich, ondanks de maatregelen die u treft, toch voordoet.
- ☐ Omschrijf welke schade er dan ontstaat of kan ontstaan voor de personen van wie u persoonsgegevens verwerkt.

Diverse maatregelen zijn denkbaar. In het onderstaande schema zijn een aantal standaard maatregelen opgenomen om u op weg te helpen. U kunt ook maatregelen vinden in bijlage 3 gekoppeld aan de vragenlijst. Maatregelen moeten in verhouding staan met het risico, de organisatie en het soort persoonsgegevens. Dit onderdeel is daarmee zeer afhankelijk van de omstandigheden.

Niveau	Maatregelen[6]
Neem maatregelen voor verwerkingen met hoge tot zeer hoge risico's.	- herstelmogelijkheid/back-up - meerfactor-authenticatie - monitoring en logging - fysieke maatregelen voor toegangsbeveiliging en toegangscontrole - dataminimalisatie - geheimhoudingsverklaringen - verwerkersovereenkomsten - screening personeel en VOG-verklaring - anonieme gegevens of pseudonimisering - rechten betrokkenen - vermijden risico's - overdragen risico's (verzekering)
Neem maatregelen voor verwerkingen met hoge tot zeer hoge risico's.	- beperken inzageniveau - transmissiecontrole - invoercontrole - transportcontrole - controle op de gegevensdragers - controle op de toegang tot apparatuur - opslagcontrole - gebruikscontrole - controle op de toegang tot gegevens - extra inzage/bezwaar mogelijkheden voor betrokkenen
Neem maatregelen voor verwerkingen met hoge tot zeer hoge risico's en midden risico's.	- project-, risico-en incidentenmanagement - data opsplitsen - integriteitscontroles - controle van toegekende bevoegdheden - privacybewustzijn-en beveiligingstrainingen - managementrapportages over risicobeheer - periodiek een audit of hack-of penetratietest uitvoeren - richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken - responsible-disclosurebeleid - service level agreements (met boeteclausules)

[6] Maatregelen van de voorgaande niveau(s) moeten ook genomen worden. Voor inspiratie of een uitwerking van de maatregel kunt u de NEN 7510, 7512 en 7513 bestuderen. Deze zijn gratis beschikbaar gesteld op internet: https://www.werkenmetnen7510.nl/.

Voorafgaand raadplegen

Zowel de hoge als zeer hoge risico's moeten afgedicht worden voordat gestart wordt met de verwerking. Lukt dit niet, dan moet u de Autoriteit Persoonsgegeven voorafgaand raadplegen. Bij een voorafgaande raadpleging geeft de AP u advies over hoe u de risico's van uw voorgenomen verwerking kunt beperken. Als u deze maatregelen uitvoert, mag u met de verwerking beginnen. Het kan ook dat de AP u adviseert om helemaal van de verwerking af te zien.

Stap 7: Rapport opstellen

De uitkomst van de DPIA legt u vast in een rapport. Alle personen betrokken bij de DPIA of de uitvoering daarvan dienen het rapport te ontvangen. Zie voor de opzet van zo'n rapport bijlage 4. Uit het rapport moet blijken hoe u alle hiervoor genoemde stappen heeft doorlopen. U kunt het rapport publiceren, dit hoeft niet. Afhankelijk van het formaat van uw organisatie moet het rapport het gepaste detailniveau bevatten. Zie daarvan een grove indicatie in het onderstaande schema.

Simpel rapport: 2000 woorden
Middel rapport: 3000 woorden
Uitgebreid rapport: 5000 woorden

Stap 8: Evaluatie

Uit de DPIA blijken risico's en te nemen maatregelen. Het is van belang dat de bedachte maatregelen ook uitgevoerd worden. Daarom moet regelmatig gecontroleerd worden of de maatregelen juist geïmplementeerd zijn en blijven. Tevens moet regelmatig gecontroleerd worden of een nieuwe DPIA nodig is.

Controleer jaarlijks of de maatregelen zijn uitgevoerd en of een nieuwe DPIA nodig is.
Controleer elk half jaar of de maatregelen zijn uitgevoerd en of een nieuwe DPIA nodig is.
Hanteer een volledige plan-do-check-act (PDCA) cyclus. Waarbij u elke twee maanden een concreet moment neemt om de maatregelen te controleren en te besluiten waar mogelijk een DPIA nodig is.

Via deze 8 stappen kunt u een DPIA doen. Na afloop heeft u beter zicht op de risico's en een middel om deze aan te pakken. Wilt u meer informatie over een DPIA dan is de volgende literatuur nuttig om te raadplegen.

Nuttige literatuur:

- NOREA, Privacy Impact Assessment (PIA), 2015.
- Rijksoverheid, Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA), 2017.
- NEN 7510, 7512, 7513.
- Groep gegevensbescherming artikel 19, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking ''waarschijnlijk een hoog risico inhoudt'' in de zin van Verordening 2016/679.
- Website Autoriteit Persoonsgegevens.

Tevens kunt u contact met Eldermans|Geerts opnemen via post@eldermans-geerts.nl of bellen naar 030-2332218.

Bijlage 1: Team

In het schema een indicatie van functionarissen die in het team opgenomen kunnen worden.

Rol / functionaris	Naam (namen)
Projectleider	
Functionaris gegevensbescherming	
Zorgaanbieder	
Security officer	
ICT-medewerker	
HRM-medewerker	
Communicatiemedewerker	
Functioneel beheerder	
Kwaliteitsmedewerker	
Financiële medewerker	
Beleidsmedewerker	
Jurist	
Medewerker facilitair	
Autorisatiebeheerder	

Bijlage 2: Documenten

Onderstaand een overzicht van de documenten ten behoeve van de documentstudie bij een DPIA. Deze opsomming is niet limitatief en er kunnen binnen de organisatie nog andere relevante documenten beschikbaar zijn. Ook kunnen de documenten zijn opgenomen in hetzelfde stuk. Voor alle niveaus geldt dat de genoemde documenten minstens aanwezig moeten zijn, inclusief de documenten uit de lagere niveaus.

Niveau	Gevraagd document	Wat is beschikbaar
Niveau 1	Verwerkingsregister	
Niveau 1	Privacyverklaring voor de cliënten van de dienstverlening	
Niveau 1	Geheimhoudingsverklaringen medewerkers, ZZP'ers en derden c.q. de (arbeids)overeenkomsten waarin deze zijn opgenomen.	
Niveau 1	Verwerkersovereenkomst(en)	
Niveau 1	Beleid en procedures i.v.m. de bewaartermijnen	
Niveau 1	Toestemmingsformulier cliënt voor het verwerken van persoonsgegevens (indien nodig)	
Niveau 2	Privacyverklaring voor de medewerkers	
Niveau 2	Beleid c.q. regels met betrekking tot het gebruik van camera's, geluidsopnames en dergelijke	
Niveau 2	Beschrijving awareness activiteiten	
Niveau 2	Samenwerkingsovereenkomsten/reglementen	
Niveau 3	Procedure afhandeling incidenten en datalekken	
Niveau 3	ICT-architectuur beschrijving en/of applicatielandschap	
Niveau 3	Procedure(s) met betrekking tot de rechten van betrokkenen	
Niveau 3	Informatiebeveiligingsbeleid en indien beschikbaar de daarbij behorende richtlijnen	
Niveau 3	Beleid c.q. regels met betrekking tot het gebruik van e-mail, WhatsApp, en andere sociale media	
Niveau 3	Autorisatiebeleid en/of autorisatiematrix (-model)	
Niveau 3	Functiebeschrijving van de FG	
Niveau 3	Functiebeschrijving van de security officer	
Niveau 4	Beschrijving/procedure voor het melden van incidenten bij een servicedesk	
Niveau 4	Jaarverslag	
Niveau 4	Implementatieplannen voor inrichting informatiebeveiliging	
Niveau 4	Implementatieplannen voor inrichting privacy	
Niveau 4	Organisatieschema en plaats van privacy en IB binnen de organisatie	
Niveau 4	Beschikbare audit- of andere onderzoeksrapportages inzake privacy en informatiebeveiliging	
Niveau 4	ICT-procedures, waaronder Change Management en Incident Management en SLA's	
Niveau 4	Inkoopvoorwaarden	
Niveau 4	Wat er op Intranet (of vergelijkbare voorziening) staat met betrekking tot privacy en informatiebeveiliging	

Bijlage 3: Vragenlijst

Zie los document.

Bijlage 4: Leeg rapport

Zie los document.