

Handboek DPIA's

Handboek DPIA's
Theorie en praktijk over DPIA's voor niet-juristen

Met praktische modellen voor
Pre-DPIA, Compacte DPIA en Uitgebreide DPIA

Mr. Francis Joung, CIPP/E
Mr. Sander van de Molen, CIPP/E

Mr. Francis Joung, CIPP/E

Mr. Sander van de Molen, CIPP/E

1e druk, september 2020

© Berghauser Pont Publishing, Amsterdam, 2020

Vormgeving omslag: Berghauser Pont Publishing

ISBN: 978-94-92952-42-4

NUR: 820

www.berghauserpont.nl

Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enig andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

No parts of this book may be reproduced in any way whatsoever without the written permission of the publisher.

Hoewel aan het maken van dit boek en de (DPIA)modellen de uiterste zorg is besteed, aanvaarden de auteurs, redacteur(en) en Berghauser Pont geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor de gevolgen hiervan. Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van art. 16h t/m 16m Auteurswet jo. het besluit van 27 november 2002, Stb. 575 dient men daarvoor de wettelijk verschuldigde vergoeding te voldoen aan de Stichting Reprorecht te Hoofddorp (Postbus 3051, 2130 KB). Redactie, auteurs en uitgever horen graag opmerkingen en suggesties van lezers. Deze kunt u sturen naar de uitgever of naar de uitgever, Danzigerkade 53, 1013 AP Amsterdam of mailen naar info@berghauserpont.nl.

Voorwoord

DPIA's spelen een cruciale rol bij het borgen van daadwerkelijke privacybescherming. Alle privacyregels ten spijt, de beste bescherming wordt in de praktijk geboden indien organisaties praktische technische en organisatorische maatregelen treffen om te voorkomen dat bepaalde risico's zich voordoen. Bijvoorbeeld door minder data te verwerken, encryptie toe te passen of door identificerende gegevens apart van de onderliggende database op te slaan, zodat bij verlies van data uit de database niet gelijk ook de identificerende gegevens op straat liggen.

Door middel van een DPIA worden systematisch alle risico's en de impact daarvan op consumenten, patiënten en burgers in kaart gebracht en wordt voor elk van de betreffende risico's beoordeeld welke mitigerende maatregelen kunnen worden toegepast. Een DPIA is in feite ook het systematisch nalopen of de AVG-beginselen van data-minimalisatie, proportionaliteit en subsidiariteit en *privacy by design* zijn toegepast. Vooral bij toepassingen van nieuwe technologieën voor dataverwerking (zoals het trainen van AI-oplossingen) is het uitvoeren van een DPIA echt een team-effort waarbij de verschillende expertises samenwerken. Hoe kun je dan bias voorkomen in AI-gestuurde oplossingen? Hoe kun je borgen dat de uitkomsten van deze AI-gestuurde toepassingen uitlegbaar zijn? Kan een beoogd doel worden bereikt op een meer privacy-vriendelijke manier? (Denk even aan de discussies rond de Corona-app ...)

In dit boek wordt veel aandacht gegeven aan zowel de theorie als de praktijk van DPIA's. Dit boek zal een nuttige bijdrage leveren om de uitvoeringspraktijk op een hoger niveau te tillen. Iets dat hard nodig is.

Prof. Lokke Moerel, advocaat Morrison & Foerster en hoogleraar Global ICT Law, Tilburg University

Inhoud

Voorwoord	V
Dankwoord	XI
Afkortingen	XV
1 Inleiding	1
2 Basisbegrippen	3
3 Theorie	7
3.1 Wat is een DPIA?	7
3.2 Waarom is een DPIA belangrijk?.....	7
3.3 Waarom eerst een Pre-DPIA?	8
3.4 Wanneer is een DPIA verplicht?	9
3.5 Stappen om na te gaan of een DPIA verplicht is	11
3.5.1 Stap 1: artikel 35 lid 3 AVG.....	11
3.5.2 Stap 2: AP-lijst	13
3.5.3 Stap 3: criteria WP29	14
3.5.4 Stap 4: zelfstandige beoordeling	14
3.5.5 Stroomschema AP wanneer DPIA verplicht	16
3.6 Wanneer hoef je geen DPIA uit te voeren?	17
3.7 Welke eisen stelt de AVG aan het uitvoeren van een DPIA?.....	18
3.8 Welke eisen stellen de WP29-richtlijnen aan het uitvoeren van een DPIA?	19
3.9 Welke DPIA-modellen zijn bruikbaar?.....	21
3.9.1 DPIA Rijksdienst.....	22
3.9.2 NOREA	22
3.9.3 DPIA-modellen buitenlandse toezichhouders	23
3.9.4 Nymity	23
3.9.5 Sectorspecifieke modellen	23
3.9.6 ISO 31000	23
3.9.7 NEN-normeringen	25
3.9.8 Het ideale model?	26
3.10 Op welk tijdstip moet een DPIA worden uitgevoerd?	27
3.11 Wie is verantwoordelijk voor de uitvoering?.....	27
3.12 Wat is de rol van de FG bij een DPIA?	27
3.13 Wat is de rol van betrokkenen bij een DPIA?	28
3.14 Wanneer moet je de AP raadplegen?.....	29
3.15 Is een DPIA een eenmalige actie?.....	30
3.16 Wat is de verhouding tussen een DPIA en de verantwoordingsplicht? 30	
3.17 Hoe verhoudt een DPIA zich tot privacy by design?	32

3.18	Is een DPIA ook relevant voor verwerkers?	33
3.19	Aanbestedingen en DPIA	34
3.20	Uitzonderingen	35
3.21	Vertrouwelijkheid van de DPIA-rapportage	35
4	Praktijk: hoe voer je een DPIA uit?	37
4.1	Totale DPIA-proces, uitgewerkt voor een uitgebreide DPIA	40
4.1.1	Start met een Pre-DPIA	40
4.1.2	Hoe ziet het Pre-DPIA-model eruit?	40
4.1.3	Wel of geen volledige DPIA?	42
4.1.4	Keuzehulp: compacte of uitgebreide DPIA? Verwerker(s) erbij betrekken?	44
4.1.5	Het DPIA-proces bij een uitgebreide DPIA	45
4.1.6	Voorfase DPIA's	46
4.1.6.1	Stappen voorfase	46
4.1.6.2	Oprichting directie/management	46
4.1.6.3	Plan van aanpak	47
4.1.6.4	De scope van de DPIA	47
4.1.6.5	De stappen bij de uitvoering van de DPIA	48
4.1.6.6	De benodigde disciplines/soorten medewerkers	48
4.1.6.7	De activiteiten die medewerkers gaan uitvoeren	49
4.1.6.8	Inschatting van de te reserveren tijd	49
4.1.6.9	Tijdplanning	49
4.1.6.10	Benodigd budget	49
4.1.6.11	DPIA uit te voeren door?	49
4.1.6.12	Rol van de FG	51
4.1.7	Uitvoering DPIA's	51
4.1.7.1	Fase uitvoering DPIA	51
4.1.7.2	Stap 1: analyse van het juridische kader	52
4.1.7.3	Stap 2: aanvullen van de vragenlijst van het model	53
4.1.7.4	Stap 3: vooraf invullen van de vragenlijst van het model	53
4.1.7.5	Stap 4: workshop	53
4.1.7.6	Stap 5: interviews	54
4.1.7.7	Stap 6: analyse antwoorden en documentatie	54
4.1.7.8	Stap 7: verder invullen van het DPIA-model	55
4.1.7.9	Stap 8: invullen memo voor DPIA-rapport	66
4.1.7.10	Stap 9: review conceptrapport	67
4.1.7.11	Stap 10: conceptrapport ter advisering voorleggen aan de FG	67
4.1.7.12	Stap 11: definitief rapport maken	68
4.1.7.13	Stap 12: rapport laten goedkeuren door directie	68
4.1.8	Wat te doen nadat het DPIA-rapport is opgeleverd (nazorgfase)?	68
4.1.8.1	Toeziens op implementatie resterende maatregelen	68
4.1.8.2	Rapport bewaren en beheren	68
4.2	Compacte DPIA	69
4.2.1	Hoe voer je een compacte DPIA uit?	69
4.2.2	Hoeveel tijd kost een compacte DPIA?	69

4.2.3	Kan ik bij vergelijkbare verwerkingen DPIA-rapporten (deels) hergebruiken?	70
4.3	DPIA in een volwassen organisatie als onderdeel van een totaal-aanpak	70
4.3.1	Waarom onderdeel van een totaalaanpak?	70
4.3.2	Hoe ziet die totaalaanpak eruit?	71
	Over de auteurs	77
	Bijlage 1: AP-lijst wanneer DPIA verplicht is.....	79
	Bijlage 2: WP29-richtlijnen voor DPIA's.....	83
	Bijlage 3: Pre-DPIA-model en toelichting	111
	Bijlage 4: Keuzehulp DPIA-model.....	119
	Bijlage 5: DPIA-model Uitgebreid en toelichting	121
	Bijlage 6: DPIA-model Compact en toelichting	137
	Bijlage 7: Inleiding rapport en managementsamenvatting.....	151
	Bijlage 8: artikel 29 van de Richtlijn (EU) 2016/680 van 27 april 2016	155
	Bijlage 9: artikel 35 AVG	157
	Bijlage 10: Bijlage uit DPIA Uitgebreid: stappen E.....	161
	Trefwoordenregister	163