DATA& PRIVACYWEB
powered by Berghauser Pont

privacyteam

CONTACT

# Themadossier AVG: DPIA

## Wat is een DPIA?

Een Data Protection Impact Assessment (DPIA) is een instrument waarmee, voorafgaand aan de verwerking van persoonsgegevens, **privacyrisico's** van een gegevensverwerking **in kaart** kunnen worden gebracht. Zo kan een organisatie passende maatregelen nemen om privacyrisico's te verkleinen.

## DPIA en de AVG

Een DPIA(1), ook wel gegevensbeschermingseffectbeoordeling, is tevens een belangrijk instrument voor organisaties om aan te kunnen tonen dat zij voldoen aan de verplichtingen van de Algemene Verordening Gegevensbescherming (AVG).(2) Het is daarbij van belang dat bij het uitvoeren van een DPIA de gevolgde methodiek en de uitkomsten worden vastgelegd in een document. Daarmee kunnen organisaties aantonen dat ze een **deugdelijke DPIA** hebben uitgevoerd, als bijvoorbeeld de Autoriteit Persoonsgegevens (AP) daar om vraagt.
In de AVG is de DPIA opgenomen in artikel 35 'Gegevensbeschermingseffectbeoordeling'. Dergelijke privacyrisico-analyses zijn **niet nieuw**. Ook onder de voorganger van de AVG, de Wet bescherming persoonsgegevens (Wbp), werden door organisaties die bewust met privacy bezig waren risico-analyses uitgevoerd op hun (belangrijke) processen.

## Wat is de functie van een DPIA?

Een organisatie wil en moet normaliter inzicht hebben in de (privacy)risico's van processen waarin data worden verwerkt. Dit is **noodzakelijk** om de **(privacy)belangen** van betrokkenen (klanten, cliënten, patiënten, burgers, leerlingen, medewerkers etc.) te kunnen beschermen. Maar ook om de eigen belangen te waarborgen. Denk hierbij aan **reputatieschade**, of aantasting van relaties met partners door privacyinbreuken. Dit inzicht wordt alleen verkregen door een inventarisatie en risicoanalyse van die processen. Dát is de functie van een DPIA. Daarmee verkrijg je inzicht en grip op de privacyrisico's van betrokkenen en de organisatie in die processen.(3)

## Wanneer een DPIA uitvoeren? Verplicht bij een hoog risicoverwerking

Onder de AVG, maar ook onder de Wet politiegegevens (Wpg) en de **Wet justitiële en strafvorderlijke gegevens (Wjsg)**, kunnen organisaties verplicht zijn om een DPIA uit te voeren. Bij processen met hoge privacyrisico's voor betrokkenen is het uitvoeren van een DPIA geen keuze maar een wettelijke verplichting. Niet nakoming van de DPIA-verplichting kan leiden tot een boete van de AP van maximaal **10 miljoen euro** of maximaal 2% van de totale wereldwijde jaaromzet van het voorgaande boekjaar, waarbij het hoogste bedrag geldt. In de boetebeleidregels van de AP is de basisboete voor het niet uitvoeren van een DPIA (terwijl deze wel verplicht is) € 310.000,-.(4)



# Themadossier AVG: DPIA- II

Aan de hand van de volgende stappen kan worden bepaald of een DPIA verplicht is:
- Stap 1: artikel 35 lid 3 AVG
- Stap 2: de lijst van de Autoriteit Persoonsgegevens
- Stap 3: de lijst van de European Data Protection Board (voorheen WP29/248)

## Verder leren

Verder leren
Praktisch aan de slag met DPIA's? Bekijk ons (online) leeraanbod:

- Handboek DPIA's, verkrijgbaar in onze bookshop
- E-learning DPIA (ontvang het handboek DPIA's gratis), zie cursusagenda
- DPIA-praktijdag (ontvang het handboek DPIA's gratis), zie cursusagenda

Het Handboek DPIA's is ook digitaal toegankelijk bij afname van een Data&Privacyweb PRO lidmaatschap. Daarmee verkrijg je toegang tot alle digitale boeken en jurisprudentie van Data&Privacyweb.

Met het Data&Privacyweb Expert lidmaatschap krijg je toegang tot de digitale versie van het Handboek DPIA en tot de E-learning DPIA. Ook kun je de DPIA-praktijkdag dan gratis volgen.

*Voetnoten*
*(1) Zie ook de richtsnoeren van de WP29 WP 248 van 4 april 2017 (en laatstelijk gewijzigd en vastgesteld op 4 oktober 2017), pagina 4: "Een gegevensbeschermingseffectbeoordeling is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken. Gegevensbeschermingseffectbeoordelingen zijn belangrijke verantwoordingsinstrumenten omdat ze verwerkingsverantwoordelijken niet alleen helpen om aan de eisen van de AVG te voldoen, maar ook om aan te tonen dat passende maatregelen zijn genomen teneinde ervoor te zorgen dat de verordening wordt nageleefd (zie ook artikel 24 AVG)."*
*(2) Een belangrijk onderscheid tussen de AVG en de vervallen Wet bescherming persoonsgegevens (Wbp), is de documentatieplicht ofwel de aantoonbaarheidsverplichting: zie artikel 5 lid 2 en artikel 24 AVG. Dit betreft de 'compliance' omtrent de verwerking van persoonsgegevens. Daarnaast geldt de verplichte PDCA-cyclus (Plan, Do, Check, Act): organisaties zullen continue moeten kunnen aantonen dat ze voldoen aan de verplichtingen van de AVG. Het is dus geen eenmalige implementatie.*
*(3) In overweging 84 van de AVG staat vermeld dat de verwerkingsverantwoordelijke of verwerker verantwoordelijk is voor het verrichten van een DPIA om met name de oorsprong, de aard, het specifieke karakter en de ernst van de risico's te evalueren. Met het resultaat van de beoordeling dient rekening te worden gehouden bij het bepalen van de passende maatregelen. Op deze wijze kan worden aangetoond dat bij de verwerking van persoonsgegevens de AVG wordt nageleefd.*
*(4) Zie: beleidsregels van 19 februari 2019.*