Smith & Doe
privacytools

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Factsheet PIA's (AVG)*

** De informatie in dit factsheet is gebaseerd op de nieuwe privacywet, de Algemene Verordening Gegevensbescherming.*

Met de nieuwe privacywet, de Algemene Verordening Gegevensbescherming (AVG) komt er voor bepaalde vormen van gebruik van persoonsgegevens ("verwerkingen") een verplichting om een Privacy Impact Assessment uit te voeren. In de AVG worden deze In de AVG worden deze "gegevensbescherming-effectbeoordelingen" genoemd.

Wat is een "PIA"?

Een PIA is een onderzoek waarbij wordt gekeken welke "stromen" persoonsgegevens er allemaal zijn, wat de daaraan verbonden risico´s zijn, hoe die risico´s kunnen worden gemitigeerd en welke maatregelen moeten worden genomen in verband met het verwerken van die persoonsgegevens.

Hoe moet een PIA er uit zien?

De AVG stelt geen specifieke eisen aan de inhoud van een PIA, dit wordt aan de markt overgelaten.

Wél staat in de AVG dat daarin **minimaal** het volgende moet worden meegenomen:

- Een **beschrijving van de verwerking** en de doeleinden daarvan en, als dat van toepassing is, de "gerechtvaardigde belangen" om de persoonsgegevens te verwerken;

Smith & Doe
privacytools

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

- Een beoordeling van de **noodzaak** en de **evenredigheid** van het verwerken van de persoonsgegevens in verhouding tot de doeleinden daarvan;
- De beoogde **maatregelen** om de risico's aan te pakken, zoals waarborgen, veiligheidsmaatregelen en mechanismen om te zorgen dat de persoonsgegevens worden beschermd en om aan te tonen dat aan de verplichtingen van de AVG wordt voldaan, met inachtneming van de rechten en belangen van de betrokken personen en eventuele andere personen.

Wanneer is het uitvoeren van een PIA verplicht?

Het uitvoeren van een PIA is verplicht bij verwerkingen die, gezien de aard, de omvang, de context en de doeleinden daarvan, een **hoog risico** met zich meebrengen.

Wanneer moet het in ieder geval?

Een PIA moet **in ieder geval** worden uitgevoerd als:

- het gaat om **grootschalig en systematische evaluatie van persoonlijke kenmerken** op basis van geautomatiseerde verwerking van de gegevens, waaronder "**uitsluitend geautomatiseerde individuele beslissingen**" die rechtsgevolgen hebben of die een andere aanzienlijke impact op de betrokken persoon, of profilering ("profiling");

- het gaat om het verwerken van bijzondere persoonsgegevens **op grote schaal**;

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

- het gaat om **systematisch monitoren** van een **publiek toegankelijke ruimte** op grote schaal.

Wanneer moet het nog meer?

Wanneer het nog meer nodig is, hangt af van verschillende omstandigheden.

De volgende omstandigheden vormen aanwijzingen voor het moeten uitvoeren van een PIA:

- als er een **nieuwe technologie** wordt gebruikt;
- als er sprake is van **bijzondere persoonsgegevens**;
- als er sprake is van "**gevoelige persoonsgegevens**" (dit zijn persoonsgegevens die een indringend beeld kunnen geven van de betrokken persoon, zoals financiële gegevens, personeelsdossiers, gegevens over uitkeringsrechten, locatiegegevens);
- als er sprake is van "**uitsluitend geautomatiseerde individuele beslissingen**", waaronder profiling, die rechtsgevolgen hebben of die een andere aanzienlijke impact op de betrokken persoon;
- als het gaat om persoonsgegevens van een **kwetsbare groep** personen, zoals kinderen of uitkeringsgerechtigden;
- als het gaat om **systematische monitoring** van de betrokken personen;
- **grootschalige** verwerkingen;
- het **koppelen** van bestanden.

Smith & Doe
privacytools

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Als er sprake is van twee of meer van de hiervoor genoemde omstandigheden, kunt u er het beste van uitgaan dat er een hoog risico is, en dus een PIA nodig.

Als er maar sprake is van één van de omstandigheden hoeft dat niet per sé, u zult dan moeten beoordelen of er niet toch sprake is van een hoog risico. Dat zal bijvoorbeeld bij bijzondere persoonsgegevens al snel het geval zijn.

Lijst van de Autoriteit Persoonsgegevens

Daarnaast heeft de Autoriteit Persoonsgegevens een lijst gepubliceerd met situaties waarin een PIA verplicht is. De lijst kunt u vinden in dit blogbericht.

Hoe vaak moet de PIA worden herhaald?

De algemene regel is dat de PIA eens in de **drie jaar** moet worden herhaald.

Maar, hier geldt ook dat als er een belangrijke wijziging is in de verwerking, bijvoorbeeld omdat het de bedoeling is om de persoonsgegevens voor andere doeleinden te verwerken, opnieuw een PIA moet worden uitgevoerd.

Let op: als uit de PIA blijkt dat het verwerken van de persoonsgegevens een verhoogd risico met zich meebrengt en uw organisatie dat risico niet adresseert of niet kan adresseren, dan moet de Autoriteit Persoonsgegevens worden gevraagd om een zogenaamd “voorafgaand onderzoek”.