AUTORITEIT PERSOONSGEGEVENS

Data protection impact assessment (DPIA)

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

In de Nederlandse vertaling van de AVG wordt de term *data protection impact assessment* (DPIA) gegevensbeschermingseffectbeoordeling genoemd.

Groot privacyrisico

Organisaties hoeven, zodra de AVG geldt, niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo als een organisatie:

systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
op grote schaal bijzondere persoonsgegevens verwerkt;
op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Buiten deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico. De Europese privacytoezichthouders hebben criteria opgesteld om het risico te bepalen. Daarnaast publiceert de Autoriteit Persoonsgegevens (AP) op termijn een lijst van verwerkingen waarvoor een DPIA verplicht is.

Guidelines DPIA

De Europese privacytoezichthouders hebben in oktober 2017 de (definitieve) Guidelines on Data Protection Impact Assessment gepubliceerd die meer uitleg geven over de DPIA. Er is ook een officiële Nederlandse vertaling van de guidelines DPIA beschikbaar.

Huidige situatie

De Rijksoverheid is nu al verplicht om bij de ontwikkeling van nieuwe wetgeving rekening te houden met de resultaten van een DPIA, nu nog Privacy Impact Assessment (PIA) genoemd. Andere organisaties zijn nu nog niet verplicht een (D)PIA uit te voeren.

Het is aan te raden om vrijwillig een (D)PIA te doen. Dit komt niet alleen de gegevensbescherming ten goede, maar ook voor de organisatie zelf levert een (D)PIA voordelen op.

Alle antwoorden op mijn vragen

Vragen over DPIA

In welke gevallen moet ik een DPIA uitvoeren?

Als verantwoordelijke moet u een *data protection impact assessment* (DPIA) uitvoeren wanneer uw gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert. Dit moet u zelf bepalen. De werkgroep van Europese privacytoezichthouders (WP29) heeft een lijst van 9* criteria opgesteld om u hierbij te helpen.

9 criteria om te toetsen of u een DPIA moet uitvoeren

Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de onderstaande 9 criteria voldoet.

1. Beoordelen van mensen op basis van persoonskenmerken

Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.

Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd.

Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium. In de aankomende WP29-guidelines over profiling volgt hierover meer uitleg.

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

5. Grootschalige gegevensverwerkingen

De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. WP29 adviseert om met de volgende criteria te bepalen of hiervan sprake is:

de hoeveelheid mensen van wie gegevens worden verwerkt;
de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
de tijdsduur van de gegevensverwerking;
de geografische reikwijdte van de gegevensverwerking.

Zie ook: wat ziet de AVG als een grootschalige verwerking van persoonsgegevens?

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

8. Gebruik van nieuwe technologieën

De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.

De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen. Sommige 'Internet of Things'-toepassingen bijvoorbeeld kunnen een grote impact hebben op het dagelijks leven en de privacy van mensen, waardoor hierbij een DPIA nodig is.

9. Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:

een recht niet kunnen uitoefenen of;
een dienst niet kunnen gebruiken of;
een contract niet kunnen afsluiten.

Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Verantwoordingsplicht

Let op: deze 9 criteria zijn een handreiking om in te schatten of u een DPIA moet uitvoeren. Ook als u aan slechts één of geen van deze criteria voldoet, moet u goed kunnen onderbouwen waarom u ervoor kiest om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht.

*In de definitieve guidelines die zijn vastgesteld in oktober 2017, is het 10e criterium 'Doorgifte van persoonsgegevens buiten de EU' vervallen. Ook legt de wet voor bestaande verwerkingen nu een link naar het 'voorafgaand onderzoek' onder de huidige privacywetgeving.

Wanneer hoef ik geen DPIA uit te voeren?

U hoeft geen *data protection impact assessment* (PIA) uit te voeren wanneer uw gegevensverwerking:

Waarschijnlijk geen hoog privacyrisico oplevert.
Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de privacytoezichthouder oordeelt dat er toch een DPIA nodig is.
Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de privacytoezichthouder de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht.

Moet ik alsnog een DPIA uitvoeren voor een bestaande verwerking?

Ja, soms moet u alsnog een *data protection impact assessment* (DPIA) uitvoeren voor een bestaande verwerking. Dat is als er iets verandert aan het risico van de gegevensverwerking. En de gegevensverwerking vervolgens (na de verandering) een hoog privacyrisico oplevert.

Geen DPIA nodig

U hoeft dus niet alsnog een DPIA uit te voeren als een van de volgende 3 situaties van toepassing is:

uw gegevensverwerking levert waarschijnlijk géén hoog privacyrisico op; *of*
u heeft voor deze verwerking al eens een voorafgaand onderzoek door de AP laten uitvoeren en de verwerking is in de tussentijd niet veranderd; *of*
de risico's van de verwerking zijn niet veranderd.

Verwerking verandert

Uw verwerking verandert bijvoorbeeld als u een nieuwe technologie gaat gebruiken. Of als u persoonsgegevens voor een ander doel gaat gebruiken. In deze situaties verandert uw gegevensverwerking feitelijk in een nieuwe gegevensverwerking. En dan kan een DPIA verplicht zijn.

Risico verandert

Verandert het privacyrisico van uw verwerking? Dan kunt u ook verplicht zijn alsnog een DPIA uit te voeren. Risico's kunnen bijvoorbeeld veranderen omdat een onderdeel van het verwerkingsproces wijzigt. De technologische ontwikkelingen gaan snel, waardoor nieuwe kwetsbaarheden kunnen ontstaan.

Omgeving verandert

Tot slot kunt u alsnog verplicht zijn een DPIA uit te voeren omdat de organisatie- of maatschappelijke context verandert. Bijvoorbeeld omdat de gevolgen van bepaalde geautomatiseerde beslissingen belangrijker zijn geworden of omdat er nieuwe categorieën mensen kwetsbaar worden voor discriminatie.

Periodieke DPIA

Vanwege de hierboven genoemde veranderingen is het sowieso aan te raden om periodiek een DPIA uit te voeren. Ook als de gegevensverwerking zelf niet is veranderd. Bijvoorbeeld een keer per 3 jaar.

Op welk moment moet ik een DPIA uitvoeren?

Start met het data protection impact assessment (DPIA) zo vroeg als praktisch gezien mogelijk is in de ontwerpfase van de gegevensverwerking. Ook als nog niet alle details van de verwerking bekend zijn. Door vroeg te beginnen, is het voor u makkelijker om aan de wettelijk vereiste principes van *privacy by design* en *privacy by default* te voldoen.

Continu proces

Let op: dat u de DPIA misschien gaandeweg moet aanpassen, is geen argument om de DPIA uit te stellen of achterwege te laten. Een DPIA uitvoeren is geen eenmalige opdracht, maar een continu proces. U zult altijd moeten (blijven) monitoren of uw gegevensverwerking wijzigt en of u daarom de DPIA moet bijstellen.

Wie moet een DPIA uitvoeren?

Als verantwoordelijke moet u ervoor zorgen dat er een *data protection impact assessment* (DPIA) wordt uitgevoerd. U moet hierbij, wanneer van toepassing, aan verschillende partijen advies vragen. U hoeft

de DPIA niet zelf uit te voeren, dit kunt u ook door iemand anders binnen of buiten uw organisatie laten doen. U blijft wel eindverantwoordelijk.

Advies FG

Is er in uw organisatie een verplichte functionaris voor de gegevensbescherming (FG) aangewezen? Dan moet u de FG om advies vragen. U moet in het rapport over de DPIA opnemen wat de FG heeft geadviseerd en wat u daarmee heeft gedaan. De FG heeft ook als taak de uitvoering van de DPIA in de gaten te houden.

Advies bewerker

Voert een bewerker (in de AVG 'verwerker' genoemd) in opdracht van u de gegevensverwerking uit? Dan moet de bewerker u ondersteunen bij het uitvoeren van de DPIA en de informatie verstrekken die u nodig heeft.

Advies betrokkenen

U moet als het nodig is de betrokkenen (de mensen van wie u gegevens wil verwerken) of hun vertegenwoordigers om hun mening vragen.

Er zijn, afhankelijk van uw specifieke situatie, verschillende geschikte manieren waarop u betrokkenen om hun mening kunt vragen. U kunt bijvoorbeeld een intern of extern onderzoek doen, consumenten- of werknemersorganisaties consulteren of uw toekomstige klanten een vragenlijst sturen.

Wijkt uw uiteindelijke beslissing af van de mening van de betrokkenen? Dan moet u uw redenen om al dan niet met de verwerking door te gaan documenteren. U moet ook uw argumentatie documenteren als u oordeelt dat het niet nodig is om de betrokkenen om hun mening te vragen.

Advies overige partijen

Tot slot is het aan te raden om vast te stellen en te documenteren welke andere partijen in uw specifieke situatie betrokken kunnen worden bij een DPIA en wat hun verantwoordelijkheden dan zijn. Bijvoorbeeld de IT-afdeling, andere afdelingen en onafhankelijke experts (zoals advocaten, technici, beveiligingsexperts, sociologen etc.).

Op welke manier moet ik een DPIA uitvoeren?

Er zijn verschillende methodes om een *data protection impact assessment* (DPIA) uit te voeren. U kunt er zelf een kiezen, als u maar aan de basisvereisten voldoet zoals die in de AVG staan beschreven.

Voorwaarden DPIA

De DPIA moet in ieder geval het volgende bevatten:

Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan. Beroept u zich op een gerechtvaardigd belang als grondslag voor de verwerking? Neem dit dan ook op in de beschrijving.

Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen. Dat houdt in: is het verwerken van persoonsgegevens op deze manier noodzakelijk op uw doel te bereiken? En is de inbreuk op de privacy van de betrokkenen (de mensen van wie u gegevens verwerkt) niet onevenredig in verhouding tot dit doel?
Een beoordeling van de privacyrisico's voor de betrokkenen.
De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat u aan de AVG voldoet.

Handreiking PIA

U vindt een handreiking voor de uitvoering van een DPIA op de website van de beroepsorganisatie van IT-auditors (NOREA).

Publicaties

4 oktober 2017
Guidelines on Data Protection Impact Assessment (DPIA)

6 november 2017
Nederlandse vertaling guidelines DPIA

Wetgevingsadvies / 6 juni 2017
Advies Toetsmodel GEB Rijksdienst