**Gegevensbeschermingseffectbeoordeling / Data Protect Impact Assessment (DPIA)**

In het kader van de AVG kunnen organisaties vanaf 25 mei 2018 verplicht zijn om privacy risico’s in kaart te brengen. EenData Protect Impact Assessment (DPIA), in het Nederlands een gegevensbeschermingseffectbeoordeling genoemd, hoeft alleen te worden opgesteld als bij verwerking van persoonsgegevens een groot privacyrisico ontstaat voor de betrokken mensen.

**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 twee of meer van de onderstaande negen criteria voldoet.

**1. Beoordelen van mensen op basis van persoonskenmerken**

Het gaat hierbij onder meer om profiling. 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](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financi%C3%ABn/kredietwaardigheid-en-schulden) 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.

**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 (), 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’. Criteria waaraan u kunt denken zijn:

* 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.

Voorbeeld: organisaties als UWV of Google verwerken op grote schaal 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.

**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.