

Scan: Is een DPIA noodzakelijk?

De European Data Protection Board (EDPB) heeft op basis van de Algemene Verordening Gegevensbescherming (AVG) vastgesteld wanneer organisaties verplicht zijn een Data Protection Impact Assessment (DPIA) uit te voeren. Aanvullend heeft de Autoriteit Persoonsgegevens (AP) ook een lijst opgesteld van verwerkingen van persoonsgegevens die mogelijk leiden tot een hoog privacyrisico. Op basis van deze criteria wordt duidelijk wanneer het uitvoeren van een DPIA verplicht is, zoals ook inmiddels is gepubliceerd in de Staatscourant¹. Deze criteria zijn in dit snelle afwegingshulpmiddel verwerkt.

Geef antwoord op de vragen in de selectievakken ja/nee. Onderaan zie je de uitkomst.
De voorbeelden bij iedere vraag helpen bij de juiste interpretatie. *Let op: er is altijd een privacycheck nodig, ook als een DPIA niet vereist is.*

Noteer hier de titel van de verwerkingsactiviteit

Er zijn 4 centrale vragen die eerst beantwoord moeten worden om te bepalen of een DPIA moet worden uitgevoerd. Om die te beantwoorden, geef je antwoord op de vragen in de selectievakken met ja/nee (klik op het pijltje van het uitklapmenu). Onderaan de lijst zie je of een DPIA nodig is.

Vraag 1 – Worden er bij de verwerkingsactiviteit persoonsgegevens verwerkt?
Als het antwoord 'nee' is, is het invullen van de scan niet nodig.

Een DPIA is verplicht als een van de deelantwoorden op vraag 2 hieronder 'ja' is.

Vraag 2 - Vul de deelantwoorden in voor de berekening van het antwoord - Staat de verwerking op de onderstaande lijst van 17 verwerkingen? Een DPIA is verplicht als een van de deelantwoorden 'ja' is.

2.1 Heimelijk onderzoek

Grootschalige verwerkingen van persoonsgegevens en/of stelselmatige monitoring waarbij informatie wordt verzameld door middel van onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen. Een gegevensbeschermingseffectbeoordeling (DPIA) is ook verplicht in geval van heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers (bij deze laatste verwerking dient ook in incidentele gevallen een gegevensbeschermings-effectbeoordeling (DPIA) te worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen de betrokkene (werknemer) en de verwerkingsverantwoordelijke (werkgever).

2.2 Zwarte lijsten

Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden.

2.3. Fraudebestrijding

Grootschalige verwerkingen en/of stelselmatige monitoring van (bijzondere) persoonsgegevens in het kader van fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.

2.4 Beoordelen van mensen op basis van persoonskenmerken en gedrag

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die leiden tot of gebruik maken van inschattingen van gedrag of eigenschappen van natuurlijke personen. 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 of de kredietwaardigheid van natuurlijke personen.

2.5 Financiële situatie

Grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden.

2.6 Genetische persoonsgegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens.

2.7 Gezondheidsgegevens

Grootschalige verwerkingen van gegevens over gezondheid. Let op: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de AVG uitgezonderd van de verplichting een DPIA uit te voeren.

2.8 Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard met elkaar uitwisselen. Bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

2.9 Cameratoezicht

Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones.

2.10 Flexibel cameratoezicht

Grootschalig en/of systematisch gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.

2.11 Controle werknemers

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren.

2.12 Locatiegegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen.

berekend resultaat

**misschien DPIA
nodig, maak de
vragen af**
(zie verantwoording
onderaan)

nover over ae
vraagnummers voor een
toelichting
antwoord 1

Ja

vraag
1

berekend resultaat

berekend veld:

Nee

antwoord 2.1

Nee

2.1

antwoord 2.2

Nee

2.2

antwoord 2.3

Nee

2.3

antwoord 2.4

Nee

2.4

antwoord 2.5

Nee

2.5

antwoord 2.6

Nee

2.6

antwoord 2.7

Nee

2.7

antwoord 2.8

Nee

2.8

antwoord 2.9

Nee

2.9

antwoord 2.10

Nee

2.10

antwoord 2.11

Nee

2.11

antwoord 2.12

Nee

2.12

2.13 Communicatiegegevens	antwoord 2.13	Nee	2.13
Grootschalige verwerkingen en/of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.			
2.14 Internet of things	antwoord 2.14	Nee	2.14
Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen.			
2.15 Profiling	antwoord 2.15	Nee	2.15
Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profiling).			
2.16 Monitoring en beïnvloeding van gedrag	antwoord 2.16	Nee	2.16
Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen wordt geobserveerd of beïnvloed, dan wel gegevens die daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behaviouraal advertising worden verzameld.			
2.17 Biometrische gegevens	antwoord 2.17	Nee	2.17
Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren. NB: Op grond van de AVG is de verwerking van biometrische gegevens met als doel de unieke identificatie van een natuurlijk persoon, in beginsel verboden. In Nederland zijn aanvullende voorwaarden gesteld in de Uitvoeringswet AVG. Enkel als de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden is de verwerking van biometrische gegevens toegestaan.			
Vraag 3 - Er is een kans dat de verwerking een hoog privacy risico voor natuurlijke personen met zich meebrengt. Hoeveel criteria uit de onderstaande verwerkingen met een mogelijk hoog privacyrisico zijn van toepassing?		berekend resultaat	
		Nee	
Is er sprake van voorgenomen verwerkingen die waarschijnlijk (gelet op hun aard, omvang, context en doeleinden) grote privacyrisico's voor de rechten en vrijheden van natuurlijke personen met zich mee brengen? Om dit te beoordelen is de volgende lijst met 9 criteria opgesteld. Kies Ja of Nee wanneer het criterium van toepassing is op de voorgenomen verwerking:			
3.1 Beoordelen van mensen op basis van persoonskenmerken (Evaluatie of scoretoekenning,	antwoord 3.1	Nee	3.1
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.			
3.2 Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg	antwoord 3.2	Nee	3.2
Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Een dergelijke 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. Voor meer informatie, zie de richtlijnen van de toezichthouder met betrekking tot wp251rev01.			
3.3 Stelselmatige en grootschalige monitoring	antwoord 3.3	Nee	3.3
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.			
3.4 Gevoelige gegevens (gegevens van zeer persoonlijke aard)	antwoord 3.4	Nee	3.4
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.			
3.5 Grootschalige gegevensverwerkingen	antwoord 3.5	Nee	3.5
De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. De Autoriteit Persoonsgegevens 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.			
3.6 Gekoppelde databases (samengevoegde datasets)	antwoord 3.6	Nee	3.6

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.

3.7 Gegevens over kwetsbare personen

antwoord 3.7

Nee

3.7

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 mogelijk niet in vrijheid toestemming kunnen geven of bezwaar maken tot het verwerken van hun gegevens, of niet in staat zijn de impact ervan te begrijpen. Het kan hierbij om bijvoorbeeld kinderen en patiënten gaan, of om werknemers, of mensen met een beperking.

3.8 Blokkering van een recht, dienst of contract voor de betrokkene

antwoord 3.8

Nee

3.8

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 of overeenkomst niet kunnen afsluiten.

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

3.9 Gebruik van nieuwe technologieën

antwoord 3.9

Nee

3.9

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.

Maar wat is nu een nieuwe technologie? De Information Commissioner's Office² (VK) zegt hierover:

"Als u van plan bent om technologie te gebruiken die u nog niet eerder hebt gebruikt- zelfs als deze technologie al eerder bestond- dan we raden u aan om toch een DPIA uit te voeren. De technologie zelf kan weliswaar al door anderen zijn getest, maar u moet ervoor zorgen dat u de risico's begrijpt en de technologie implementeert op de meest privacy-vriendelijke manier. Ook kan technologie nog steeds als een 'nieuwe technologie' worden beschouwd wanneer u bestaande technologie op een nieuwe of innovatieve manier zult inzetten. U kunt misschien in zekere mate vertrouwen op eerdere DPIA's die door de ontwikkelaar of door een andere verwerkingsverantwoordelijke al eerder is gebruikt, maar dan is het belangrijke dit wel toe te voegen aan de gegevensbeschermingseffectbeoordeling van uw eigen implementatieplannen, inclusief de specifieke aard, reikwijdte, doelen en context van uw verwerking. Wat als nieuwe technologie wordt beschouwd varieert van sector tot sector en is afhankelijk van de rijsheid van het gebruik hinnen het specifieke toepassingsgebied "

Eerder opgedane ervaringen en beveiligingsmaatregelen bepalen de context op basis waarvan te gebruiken technologie als nieuw moet worden beschouwd.

Vraag 4 – Is de verwerking al eerder als geheel of als onderdeel onderwerp van een eerdere DPIA geweest èn zijn er sindsdien geen wijzigingen in de verwerkingen, specifieke verwerkingsdoelen geweest en zijn er geen nieuwe technologieën nodig?*

antwoord 4

Ja

4

* Vul 'ja' in als de verwerking verder ongewijzigd is

Vraag 5 - DPIA-vragen afgerond? (pas 'ja' aanklikken als je klaar bent)

antwoord 5

Nee

5

Uitslag: wel/geen DPIA noodzakelijk?

Eindresultaat/advies

misschien DPIA nodig, maak de vragen af

Dit is een indicatie. Maar maak de overweging ook altijd nog op basis van gezond verstand. Het kan in sommige gevallen toch verstandig zijn een DPIA uit te voeren als dat niet verplicht is. Documenteer de afweging hieronder.

Beargumenteer hier de afweging om de DPIA wel of niet uit te voeren en archiveer deze scan voor eventuele audits.

Bronnen:

¹ Staatscourant Nr.64418/ 27 november 2019

² Information Commissioner's Office - de Engelse autoriteit voor persoonsgegevens

* De voorbeelden zijn deels afkomstig van DPIA pre-screening van Consideratie