

## DPIA of niet?





## Inhoud

0.	Inleiding	3
1.	Staat de verwerking op de lijst waarvoor een DPIA verplicht is?	3
2.	Is er sprake van een verplicht geval uit artikel 35 lid 3 AVG?	4
3.	Levert de verwerking waarschijnlijk een hoog risico op?	4
4.	Is er al een DPIA uitgevoerd?	5
5.	Checklist	5
6.	Bijlage 1. Swimlanes DPIA	7



## 0. Inleiding

Artikel 35 van de Algemene verordening gegevensbescherming (hierna: 'AVG') stelt dat in een aantal gevallen een gegevensbeschermingseffectbeoordeling nodig is. De Engelse term hiervoor is Data Protection Impact Assessment (hierna: 'DPIA'). In dit protocol staat omschreven in welke gevallen een DPIA moet worden uitgevoerd en wat een dergelijk assessment inhoudt. Aan het eind van dit protocol staat een korte checklist die kan worden doorlopen om te bepalen of er wel of geen DPIA nodig is.

Een DPIA is dus een analyse op basis waarvan bepaald wordt welke maatregelen getroffen moeten worden om de persoonsgegevens die gebruikt worden in een verwerking te beschermen. **Persoonsgegevens** zijn alle gegevens op basis waarvan je een natuurlijk persoon kan identificeren (direct of indirect), zie artikel 4 sub 1 AVG. Een **verwerking** is een al dan niet geautomatiseerde bewerking of reeks van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens (artikel 4 sub 2 AVG). Het begrip 'verwerken' is dus erg ruim en betekent eigenlijk alles wat met persoonsgegevens gedaan wordt.

Een DPIA moet worden uitgevoerd door de verwerkingsverantwoordelijke. Als de Provincie dus slechts verwerker is, hoeft zij geen DPIA uit te voeren. Een **verwerkingsverantwoordelijke** is de partij die het doel en de middelen van de verwerking vaststelt (artikel 4 sub 7 AVG). Een **verwerker** is de partij die ten dienst van een ander persoonsgegevens verwerkt (artikel 4 sub 8 AVG). De verwerker en de verwerkingsverantwoordelijke kunnen dezelfde partij zijn, maar dat hoeft niet. Daarnaast kunnen er ook meerdere verwerkingsverantwoordelijken zijn, die dan een gezamenlijke verantwoordelijkheid hebben (artikel 26 AVG).

De vragen die gesteld moeten worden om te bepalen of een DPIA nodig is zijn de volgende:

1. Staat de verwerking op de lijst waarvoor een DPIA verplicht is?
2. Is er sprake van een verplicht geval uit artikel 35 lid 3 AVG?
3. Levert de verwerking waarschijnlijk een hoog risico op?
4. Is er al een DPIA uitgevoerd?

Als u op basis van dit protocol tot de conclusie komt dat er een DPIA moet worden uitgevoerd, neem dan contact op met de privacy ambassadeur. Deze kan op zijn/haar beurt contact op nemen met de privacy coördinator en samen zullen zij zich verdiepen in de DPIA.

### 1. Staat de verwerking op de lijst waarvoor een DPIA verplicht is?

Op grond van artikel 35 lid 4 AVG heeft de Autoriteit Persoonsgegevens (hierna: 'AP') een lijst vastgesteld van verwerkingen waarvoor een DPIA verplicht is.<sup>1</sup> Het gaat in deze lijst altijd om grootschalige verwerkingen of stelselmatige monitoring van persoonsgegevens. Als de verwerking op deze lijst staat, moet er een DPIA worden uitgevoerd. Op de lijst staan de volgende verwerkingen:

Verplichte DPIA lijst AP		
1.	Heimelijk onderzoek	
2.	Zwarte lijsten	Als men zwarte lijsten opstelt op basis waarvan men ergens geen toegang meer heeft of men een recht verliest
3.	Fraudebestrijding	
4.	Creditscores	Verwerkingen op basis waarvan de kredietwaardigheid van natuurlijke personen worden geschat
5.	Financiële situatie	Verwerkingen op basis waarvan de inkomens-/vermogenspositie of het bestedingspatroon van natuurlijke

<sup>1</sup> Deze lijst heeft de AP op 27 november 2019 vastgesteld.



personen wordt afgeleid		
6.	Genetische persoonsgegevens	
7.	Gezondheidsgegevens	
8.	Samenwerkingsverbanden	Gevallen waarin men in een samenwerkingsverband persoonsgegevens deelt
9.	Cameratoezicht	
10.	Flexibel cameratoezicht	
11.	Controle werknemers	
12.	Locatiegegevens	
13.	Communicatiegegevens	
14.	Internet of things	Verwerkingen die worden gegenereerd door apparaten die verbonden zijn met het internet of via het internet gegevens versturen of uitwisselen
15.	Profilering	
16.	Observatie en beïnvloeding van gedrag	
17.	Biometrische gegevens	

## 2. Is er sprake van een verplicht geval uit artikel 35 lid 3 AVG?

Naast de lijst van de AP zijn er drie gevallen wanneer een DPIA verplicht is, die volgen uit artikel 35 lid 3 AVG:

- a. een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen die is gebaseerd op een geautomatiseerde verwerking;
- b. grootschalige verwerking van bijzondere categorieën van persoonsgegevens;
- c. stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Bij sub a is van belang dat er op grond van de verwerking ter beoordeling van persoonlijke aspecten een besluit wordt genomen waaraan rechtsgevolgen zijn verbonden die gevolgen hebben voor de natuurlijke persoon. Profilering valt hier ook onder.

Om te bepalen wat onder de bijzondere categorieën van persoonsgegevens van sub b valt moet worden gekeken naar artikel 9 lid 1 AVG. Het betreffen gegevens omtrent de etnische afkomst, politieke opvattingen, religie, genetische gegevens, gegevens over gezondheid, seksuele oriëntatie of lidmaatschap van een vakbond. De verwerking van gegevens betreffende strafrechtelijke informatie mogen alleen verwerkt worden indien dat noodzakelijk is en geregeld is in een wet (artikel 10 AVG).

Bij sub c moet met name worden gedacht aan cameratoezicht in openbaar toegankelijke ruimten, maar ook andere methoden van bewaking waarbij persoonsgegevens worden verwerkt.

## 3. Levert de verwerking waarschijnlijk een hoog risico op?

Als de verwerking niet op de verplichte lijst van de AP staat en er geen sprake is van een verplicht geval op grond van artikel 35 lid 3 AVG, moet worden beoordeeld of de verwerking waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen (artikel 35 lid 1 AVG). Om te bepalen of er 'waarschijnlijk een hoog risico' is, hebben de Europese privacy toezichthouders een lijst opgesteld met 9 criteria. Als de verwerking aan 2 of meer van deze criteria voldoet, moet een DPIA worden uitgevoerd:



9 criteria van de Europese toezichthouders	
1. Beoordelen van mensen op basis van persoonskenmerken	Profilering of scoretoekenning op basis van bepaalde eigenschappen
2. Geautomatiseerde beslissingen	Geautomatiseerde verwerking met daadwerkelijke gevolgen voor betrokkenen.
3. Stelselmatige en grootschalige monitoring	Verwerking om betrokkenen te observeren/monitoren of controleren
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard	Zie de lijst van artikel 9 lid 1 en artikel 10 AVG
5. Grootschalige gegevensverwerkingen	Met grootschalig wordt bedoeld: veel personen, veel gegevens, langdurige verwerking of een geografisch groot gebied
6. Gekoppelde databases	Gegevens die uit verschillende databases (met verschillende doelen) worden gekoppeld
7. Gegevens over kwetsbare personen	Het gaat hier om machtsongelijkheid. Denk bij kwetsbare personen aan: kinderen, werknemers, bejaarden, geestelijk gehandicapten of asielzoekers
8. Gebruik van nieuwe technologieën	
9. Blokkering van een recht, dienst of contract	

Het is ook mogelijk dat de verwerking slechts aan een van deze criteria voldoet (of aan geen), maar dat men toch denkt dat een DPIA nodig kan zijn. In geval van twijfel, neem contact op met het cluster JZI!

#### 4. Is er al een DPIA uitgevoerd?

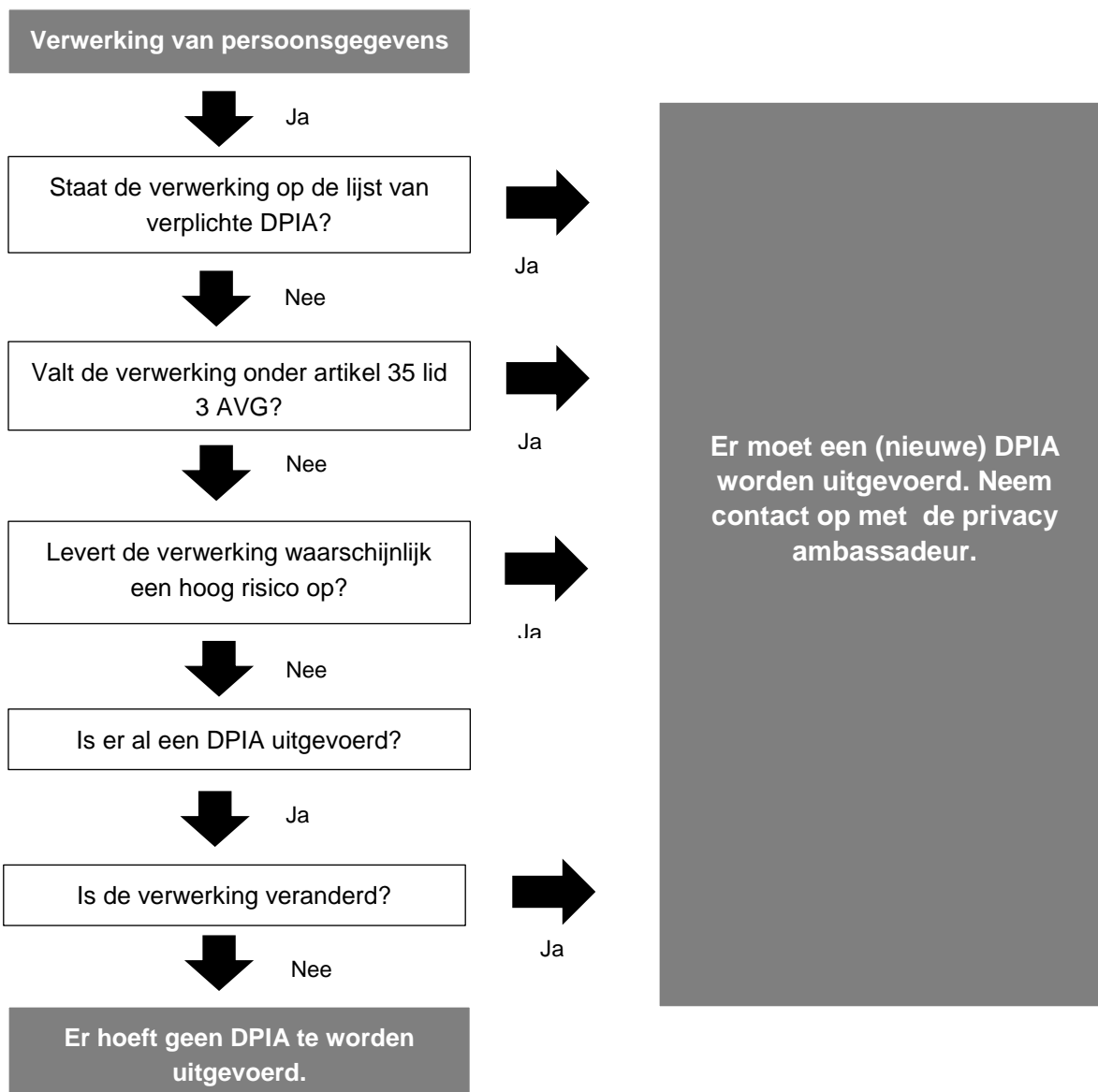
Er hoeft niet voor elke nieuwe verwerking die voldoet aan een van de bovenstaande criteria een DPIA uitgevoerd te worden. Het is namelijk mogelijk dat er al een DPIA voor een vergelijkbare verwerking is uitgevoerd of dat op Europees of nationaal niveau al een DPIA voor deze verwerking is uitgevoerd. Als u denkt dat een DPIA moet worden uitgevoerd, meld dit dan bij de privacy ambassadeur. Deze zal nagaan of dit inderdaad nodig is en of er al een eerdere DPIA is uitgevoerd die ook van toepassing is op deze verwerking.

#### 5. Checklist


Op de volgende pagina staat een stappenplan met de vier hiervoor besproken vragen. Aan de hand van dit protocol kan men dus bepalen of een DPIA moet worden uitgevoerd. Dit protocol kan zowel gebruikt worden bij nieuwe verwerkingen, als bij verwerkingen die nu al uitgevoerd worden. Belangrijk om te onthouden is dat de verwerkingsverantwoordelijke de DPIA moet uitvoeren en dus ook moet bepalen of een DPIA nodig is. Voordat aan het stappenplan wordt begonnen moet dus eerst worden vastgesteld dat:

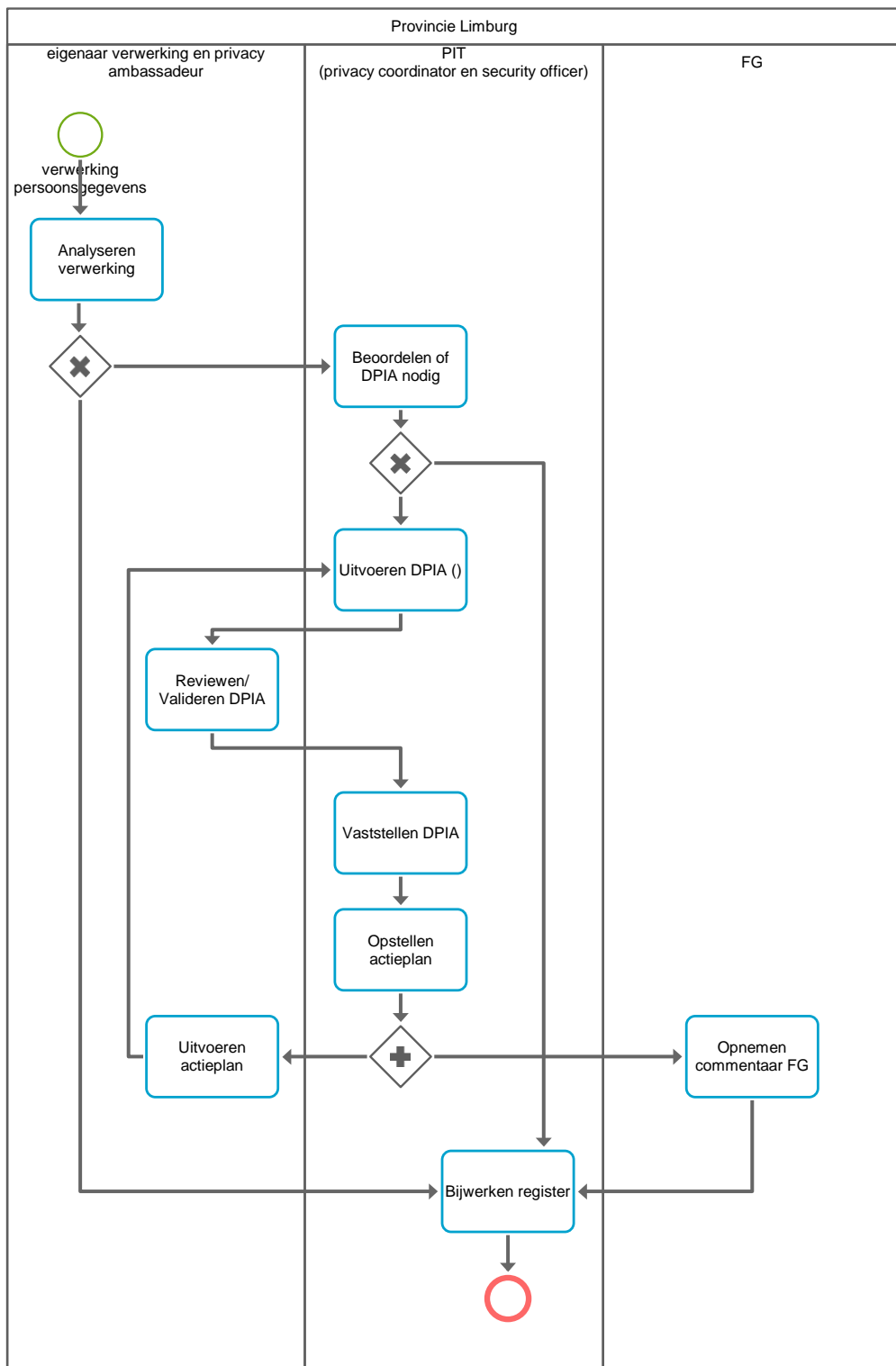
1. het **persoonsgegevens** betreft;
2. die **verwerkt** worden;
3. de Provincie de **verwerkingsverantwoordelijke** is.

In de inleiding staan de definities van deze begrippen. Nogmaals: neem bij vragen of twijfel contact op met de privacy ambassadeur.



## 6. Bijlage 1. Swimlanes DPIA

<p>Naam: Uitvoeren DPIA</p> <p>Type: BPMN-samenwerkingsdiagram (BPMN 2.0)</p>	<p>provincie limburg </p> <p>Maker: <span style="background-color: black; color: black;">XXXXXXXXXX</span></p> <p>Laatste wijziging: 22-jan-2020 9:28:38</p>
---	---



**Naam**

Uitvoeren DPIA

**Beschrijving**

Aan de hand van het protocol DPIA wordt beoordeeld of met betrekking tot een verwerking van persoonsgegevens, een data privacy impact analyse (DPIA) gemaakt moet worden.

Elke verwerking van persoonsgegevens (hoe minimaal dan ook) dient opgenomen te worden in het register van "verwerkingen van persoonsgegevens". In het register wordt tevens opgenomen of er DPIA is uitgevoerd of niet. Indien geen DPIA wordt uitgevoerd wordt de reden opgenomen in het register, In de meeste gevallen zal de reden zijn dat dit nodig is volgens het protocol DPIA.

Taak		Omschrijving
	Uitvoeren actieplan	De eigenaar van de registratie draagt zorg dat het actieplan wordt opgepakt en wordt uitgevoerd. Maatregelen kunnen betrekking hebben op de procedures binnen de eigen processen maar kunnen ook buiten de eigen invloedssfeer liggen. In dit laatste geval zal met de betreffende clusters (voornamelijk O&I, FD en P&O) afstemming moeten plaatsvinden.
R	diverse functionarissen, afhankelijk van maatregelen	
A	eigenaar registratie	
S	diverse functionarissen	
C		
I	privacycoördinator, information security officer, functionaris gegevensbescherming	
	Reviewen/ Valideren DPIA	Het DPIA document (resultaat van het uitvoeren van de DPIA) wordt gereviewed en beoordeeld. Eventuele aanpassingen worden doorgegeven aan de privacy coördinator.
R	eigenaar registratie, privacy ambassadeur	
A	eigenaar registratie	
S	privacycoördinator	
C		
I	privacycoördinator, information security officer	
	Analyseren verwerking	Aan de hand van het protocol DPIA wordt nagegaan of voor de betreffende registratie van persoonsgegevens een DPIA nodig is. Is dit het geval dan neemt de privacy ambassadeur contact op met de privacycoördinator bij JZI. Is dit niet het geval dan wordt de registratie gemeld bij de privacycoördinator en wordt aangegeven dat geen DPIA nodig is.
R	privacy ambassadeur	
A	eigenaar registratie	
S		
C	privacycoördinator	



Taak		Omschrijving
I		
	Uitvoeren DPIA ()	De privacycoördinator en de information security officer voeren de DPIA uit waarbij de eigenaar van de verwerking en de privacy ambassadeur zorg dragen voor de inhoudelijke informatie. De betreffende informatie wordt vastgelegd in het DPIA-tool van de IBD. De betreffende informatie komt in de vorm van een PDF-document beschikbaar.
R	privacycoördinator, information security officer	
A	eigenaar registratie	
S	functionaris gegevensbescherming	
C	eigenaar registratie, privacy ambassadeur	
I		
	Opstellen actieplan	Aan de hand van de analyse wordt gekeken welke additionele maatregelen nodig zijn om eventuele risico's te minimaliseren. Deze worden opgenomen in een actieplan.
R	information security officer, privacycoördinator	
A	eigenaar registratie	
S		
C	eigenaar registratie, privacy ambassadeur	
I	functionaris gegevensbescherming	
	Vaststellen DPIA	Binnen het PIT wordt de DPIA vastgesteld.
R	privacycoördinator, information security officer	
A	eigenaar registratie	
S		
C		
I	functionaris gegevensbescherming	
	Bijwerken register	Het register van persoonsregistraties wordt bijgewerkt aan de hand van informatie uit de voorgaande activiteiten.
R	privacycoördinator	
A	privacycoördinator	
S	information security	

Taak		Omschrijving
	officer	
C	privacy ambassadeur	
I	functionaris gegevensbescherming	
	Opnemen commentaar FG	Aan de hand van de uitgevoerde analyse wordt het commentaar van de FG opgenomen bij de analyse (wordt opgenomen in het DPIA tool van de IBD).
R	functionaris gegevensbescherming	
A	functionaris gegevensbescherming	
S		
C		
I	eigenaar registratie, privacy ambassadeur, privacycoördinator, information security officer	
	Beoordelen of DPIA nodig	De privacycoördinator beoordeelt a.d.h.v. het protocol DPIA of er (echt) een DPIA nodig is. Is dit niet het geval dan wordt de betreffende registratie opgenomen in het register en aangegeven dat o.b.v. het protocol geen DPIA nodig is. Is dit wel het geval dan wordt de betreffende registratie geagendeerd in het PIT en wordt de information security officer geïnformeerd.
R	privacycoördinator	
A	eigenaar registratie	
S		
C	privacy ambassadeur	
I	information security officer	