DPIA

EISEN & UITVOERING

Versie 1.0
Mariam Bagramjan

Cuccibu, auteur Mariam Bagramjan
CucciBook DPIA

Uitgegeven door Cuccibu, Nederland

INHOUDSOPGAVE

Inhoud

INTRODUCTIE

Bepaalde verwerkingen van persoonsgegevens kunnen vanwege hun aard of grootschaligheid een hoog risico voor de rechten en vrijheden van de betrokkenen opleveren. Het is in dat geval van belang om aanvullende maatregelen te nemen om de hoogste risico's weg te nemen of in ieder geval zodanig te mitigeren dat er niet meer van hoge risico's voor de bescherming van persoonsgegevens kan worden gesproken. In gevallen van een hoog risico geldt op grond van artikel 35 van de Algemene Verordening Gegevensbescherming (AVG) de verplichting voor het uitvoeren van een zogenaamde gegevensbeschermingseffectenbeoordeling, ook wel een Data Protection Impact Assessment (DPIA) genoemd.

In dit informatieboekje leggen wij uit wat een DPIA is, welke eisen hieraan gesteld worden, wanneer een DPIA verplicht is en hoe deze uitgevoerd dient te worden.

Reduce Risk, Create Value!

DPIA

Wat is een DPIA?
Een DPIA is een beoordeling van de verwerking van de persoonsgegevens, waarbij wordt gekeken naar de consequenties en risico's voor de betrokkenen die de verwerking van de persoonsgegevens met zich meebrengt. Een goed moment om het DPIA uit te voeren is wanneer er een concreet voornemen is om persoonsgegevens te gaan verwerken of bestaande verwerkingen aan te passen/uit te breiden.

Het doel van een DPIA is om een beeld te krijgen van de eventuele risico's voor de bescherming van de persoonsgegevens van betrokkenen en veel breder, namelijk hun fundamentele rechten en vrijheden. Wanneer de risico's in beeld zijn gebracht, kan dan worden bepaald welke maatregelen genomen moeten worden om de risico's te verzachten.

Een DPIA is overigens niet voor elke verwerking een vereiste. In welke gevallen je wel en in welke gevallen je juist niet verplicht bent om een DPIA uit te voeren, wordt hieronder uitgelegd.

Verplichte DPIA's
Artikel 35 AVG schrijft voor dat wanneer een verwerking (waarschijnlijk) een hoog risico voor fundamentele rechten en vrijheden oplevert, de uitvoering van een DPIA verplicht is en de mitigatie van de hoge risico's een voorwaarde is om met de verwerking van persoonsgegevens te starten. Uit lid 3 van dit artikel volgt dat een DPIA in elk geval vereist is wanneer er sprake is van:

- Systematische en uitvoerige beoordeling van persoonlijke aspecten van natuurlijke personen, waaronder profilering;
- Grootschalige verwerking van bijzondere categorieën van persoonsgegevens of strafrechtelijke gegevens;
- Grootschalige en stelselmatige monitoring van openbaar toegankelijke ruimten (denk aan cameratoezicht).

Europese lijst met criteria
Naast deze drie gevallen heeft de Artikel 29-Werkgroep, een adviesorgaan dat adviseerde aan de Europese Commissie en de voorloper is van de EDPB[1], een lijst met negen criteria[2] opgesteld aan de hand waarvan kan worden beoordeeld of er sprake is van een hoog privacyrisico. Wanneer aan twee of meer van de hieronder genoemde criteria wordt voldaan, kan niet worden ontkomen aan de verplichte uitvoering van een DPIA:

1. De verwerking bestaat uit de beoordeling van mensen op basis van persoonskenmerken: denk hierbij aan profilering;
2. Op basis van de aanwezige persoonsgegevens worden beslissingen genomen die rechtsgevolgen voor betrokkenen kunnen hebben. Het gaat daarbij om beslissingen die geautomatiseerd zijn

[1] Dit is een onafhankelijk orgaan waarin alle nationale privacytoezichthouders uit de EU samenwerken. Dit orgaan zorgt ervoor dat de AVG en de Richtlijn gegevensbescherming consequent toegepast worden in de EU.

[2] Artikel 29-Werkgroep, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev.01), 4 April 2017.

genomen. Dat wil zeggen dat er geen menselijke tussenkomst is geweest.
3. De gegevensverwerking betreft een stelselmatige en grootschalige monitoring zoals de monitoring van het gedrag van medewerkers op basis van strakke loggings en controle op loggings;
4. De voorgenomen verwerking van persoonsgegevens betreft bijzondere persoonsgegevens zoals bijvoorbeeld gegevens over de gezondheid;
5. Er is sprake van grootschalige gegevensverwerkingen: hierbij is het aantal betrokkenen, het aantal persoonsgegevens, de tijdsduur en de geografische reikwijdte van belang;
6. Diverse databases worden aan elkaar gekoppeld waardoor er in feite diverse gegevens bij elkaar worden gebracht;
7. De voorgenomen gegevensverwerking betreft een kwetsbare groep personen, zoals kinderen;
8. Bij de voorgenomen verwerking wordt gebruik gemaakt van nieuwe technologieën, zoals 'Internet of Things';
9. De verwerking leidt ertoe dat een recht, dienst of contract van de betrokkene wordt geblokkeerd.

Nationale lijst met criteria[3]

Naast deze lijst van Artikel 29-Werkgroep is er ook op nationaal niveau een lijst opgesteld door de Autoritiet Persoonsgegevens (hierna: AP) van de soorten verwerkingen waarvoor de uitvoering van een DPIA verplicht is. Ook andere landen hebben zo'n lijst opgesteld. Echter, in de lijsten zitten verschillen. Het is daarom van belang om na te gaan welke gevallen er opgenomen zijn in de lijst[en] van de land[en] waar de verwerking plaats zal vinden. De volgende gevallen zijn opgenomen in de lijst die de AP heeft opgesteld:

1. De uitvoering van een heimelijk onderzoek. Dit wil zeggen dat persoonsgegevens over een betrokkene worden verzameld zonder dat de betrokkene hiervan op de hoogte is;
2. Opnemen van betrokkenen in zwarte lijsten. Het gaat bijvoorbeeld om lijsten die over onrechtmatig gedrag van werknemers gaan;
3. Gegevensverwerking ten behoeve van fraudebestrijding door bijvoorbeeld sociale diensten;
4. Het toekennen van creditscores aan bepaalde betrokkenen;
5. Gegevensverwerkingen betreffende de financiële situatie van de betrokkene, denk bijvoorbeeld aan overzichten van bankoverschrijvingen;
6. Verwerking van genetische persoonsgegevens zoals DNA-analyses voor het in kaart brengen van persoonlijke kenmerken;
7. Verwerking van gezondheidsgegevens, bijvoorbeeld door onderwijsinstellingen;
8. Verwerkingen van persoonsgegevens in samenwerkingsverbanden, bijvoorbeeld wanneer meerdere organisatie gezamenlijk het doel en de middelen van de verwerking bepalen en persoonsgegevens met elkaar delen;
9. Uitvoering van cameratoezicht bijvoorbeeld in openbare ruimtes;

[3] Besluit van de Autoriteit Persoonsgegevens van 27 november 2019 (*Stcrt.* 2019, 64418).

10. Uitvoering van flexibel cameratoezicht bijvoorbeeld wanneer waarbij camera's op kleding of helm van brandweer- of ambulancepersoneel worden geplaatst;
11. Gegevensverwerking ten behoeve van controle van werknemers, bijvoorbeeld het (stelselmatig) opvragen van e-mail en internetgebruik van medewerkers;
12. Verwerking van locatiegegevens, bijvoorbeeld door navigatiesystemen;
13. Verwerking van communicatiegegevens;
14. Gegevensverwerking door middel van internet of things, bijvoorbeeld verwerking van persoonsgegevens door slimme televisies of slimme huishoudelijke apparaten;
15. Profilering bijvoorbeeld door beoordeling van beroepsprestaties;
16. Observatie en beïnvloeding van gedrag.
17. Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.

Niet verplichte DPIA'S

Je bent niet verplicht om een DPIA uit te voeren wanneer:

- De verwerking naar alle waarschijnlijkheid geen hoog risico inhoudt;
- De verwerking sterk lijkt op een verwerking waarvoor eerder al een DPIA is uitgevoerd;
- De verwerking plaatsvindt op basis van een Europese of andere nationale wet en bij de totstandkoming van die wet al een DPIA is uitgevoerd; of
- De verwerking op een lijst staat waarvoor het uitvoeren van een DPIA niet verplicht is. Privacytoezichthouders hebben op grond van de AVG de mogelijkheid om zo'n lijst op te stellen; dit is echter niet verplicht. De AP heeft een dergelijke lijst niet opgesteld.

UITVOERING EN INHOUD

Uitvoering DPIA
Met de uitvoering van een DPIA dient zo vroeg mogelijk in het proces van de verwerking te worden gestart. De verwerkings-verantwoordelijke zorgt voor de uitvoering van de DPIA en kan de uitvoering zelf doen of laten uitvoeren door een derde. Een DPIA wordt in de praktijk dan ook meestal door de proceseigenaren uitgevoerd met de steun van de Privacy Officer (PO) in de organisatie. De Functionaris Gegevensbescherming (FG) is in ieder geval niet de persoon om een DPIA uit te voeren. Dit heeft te maken met het feit dat een FG juist een toezichthoudende en adviserende rol heeft. De FG zal dan ook op het DPIA-rapport een advies moeten schrijven.[4]

Hoe een DPIA moet worden aangepakt is niet bij wet voorgeschreven. Dat zal per organisatie en per verwerking verschillen. Het is echter raadzaam om binnen de organisatie een procedure omtrent de uitvoering van een DPIA op te stellen waarin in ieder geval de volgende zaken terugkomen:

- Voorwaarden (en beleid eigen organisatie) uitvoering DPIA's;
- De specifieke verwerkingen binnen de organisatie waar in ieder geval een DPIA voor moet worden uitgevoerd;
- Moment uitvoering DPIA;
- Verantwoordelijke functionaris voor de uitvoering van de DPIA;
- Aanpak, tijdslijn en verdeling verantwoordelijkheden;
- Advisering op uitvoering en uitkomsten DPIA;
- Besluitvorming omtrent de uitkomsten van de DPIA;
- Evaluatie van de procedure;
- Herhaling van DPIA's;
- Rapportagelijnen;
- Rapportagekeuze;
- Bijlagen met vragenlijsten als men ervoor kiest om met een standaard vragenlijst te werken;
- Nog meer relevante procedurele zaken afhankelijk van de organisatie.

De procedure rondom de DPIA zal in ieder geval duidelijk en herhaalbaar moeten zijn voor de organisatie. Het wiel hoeft niet steeds opnieuw te worden uitgevonden.

Rapportage DPIA
Er zijn diverse templates voor zowel DPIA-vragen als DPIA-rapportages. Zo heeft NOREA vragenlijsten gepubliceerd die binnen veel gemeenten als basis worden gebruikt. De Rijksoverheid heeft ook een Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) gepubliceerd waar de meeste organisaties gebruik van maken om de DPIA-uitkomsten te rapporteren. De verwerkingsverantwoordelijk is vrij in de keuze van de uitvoering en rapportage van de DPIA, zolang er maar aan de basisvereisten voor een DPIA uit artikel 35 lid 7 AVG wordt voldaan.

In ieder geval zal een DPIA-rapportage moeten bevatten:

- Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;

[4] Artikel 39 lid 1 sub c AVG.

- De belangen die voor de verwerkingsverantwoordelijke aanwezig zijn om de verwerking plaats te laten vinden en waarom die belangen gerechtvaardigd zouden zijn voor de verwerking;
- Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen;
- Een beoordeling van de risico's voor de betrokkenen;
- Beoogde maatregelen om de risico's aan te pakken en aan te tonen dat is voldaan aan de AVG.

Niet een vereiste op basis van artikel 35 AVG maar zeker daarmee niet onbelangrijk is de toelichting en onderbouwing van:

- De grondslagen van de verwerking;
- De beoogde bewaartermijnen en de beoordeling van de termijnen op basis van wet en noodzaak;
- De betrokken partijen bij de verwerking, hun rol in de verwerking en de afspraken die met deze partijen eventueel zijn gemaakt;
- De reeds genomen maatregelen om risico's te verkleinen;

Uitkomsten DPIA

De uitvoering van een DPIA kan leiden tot drie verschillende uitkomsten. Zo kan het zijn dat na de uitvoering van de DPIA blijkt dat de beoogde gegevensverwerking geen groot risico voor de betrokkenen oplevert. In dat geval kan de verwerking onbelemmerd plaatsvinden als de FG hier ook positief over heeft geadviseerd.

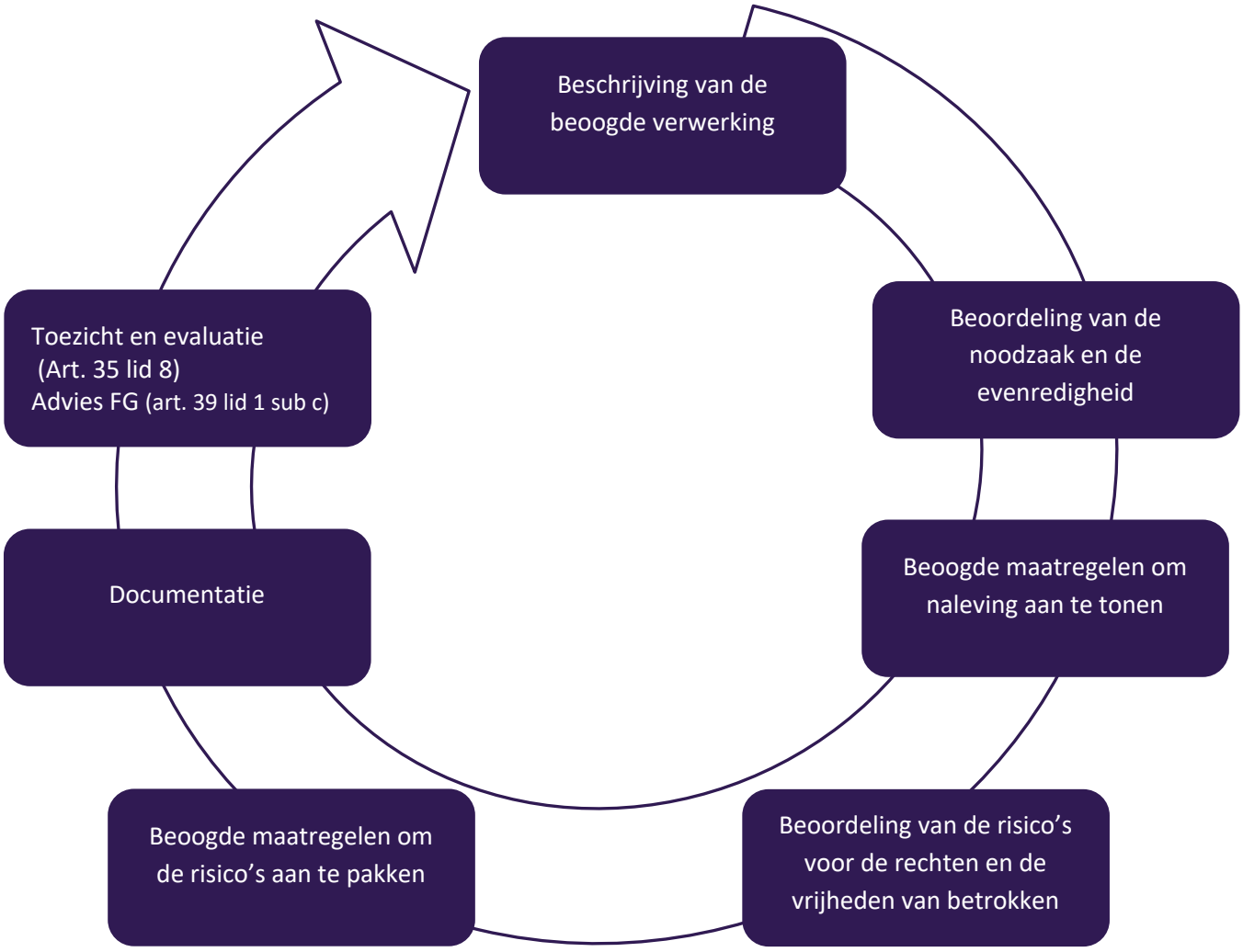
Verder kan het zo zijn dat de beoogde gegevensverwerking wel een groot privacyrisico voor de betrokkene oplevert, maar dat dit risico voorkomen kan worden door het nemen van risciobeperkende maatregelen. In dat geval kan de FG adviseren over de te nemen maatregelen. Uiteindelijk zal de (eind)verantwoordelijke van het proces waar de verwerking deel van uitmaakt, een besluit hierover nemen.

Tot slot kan het voorkomen dat de beoogde gegevensverwerking een groot risico voor de betrokkenen oplevert en dat dit risico niet door risicobeperkende maatregelen kan worden gemitigeerd of weggenomen. In dat geval schrijft de AVG voor dat de AP voorafgaand aan de verwerking moet worden geraadpleegd.

DPIA: EEN CONTINU PROCES

Het uitvoeren van een DPIA is een doorlopende verplichting. In de gevallen waar bijvoorbeeld de verwerking, de privacyrisico's of context van de verwerking veranderd zijn, verandert de gegevensverwerking in een nieuwe verwerking en kan een nieuwe DPIA verplicht zijn. Aangezien de verwerkingen gedurende de tijd kunnen veranderen, wordt door de AP aangeraden om op dezelfde verwerking periodiek een DPIA uit te voeren, bijvoorbeeld eenmaal per drie jaar.

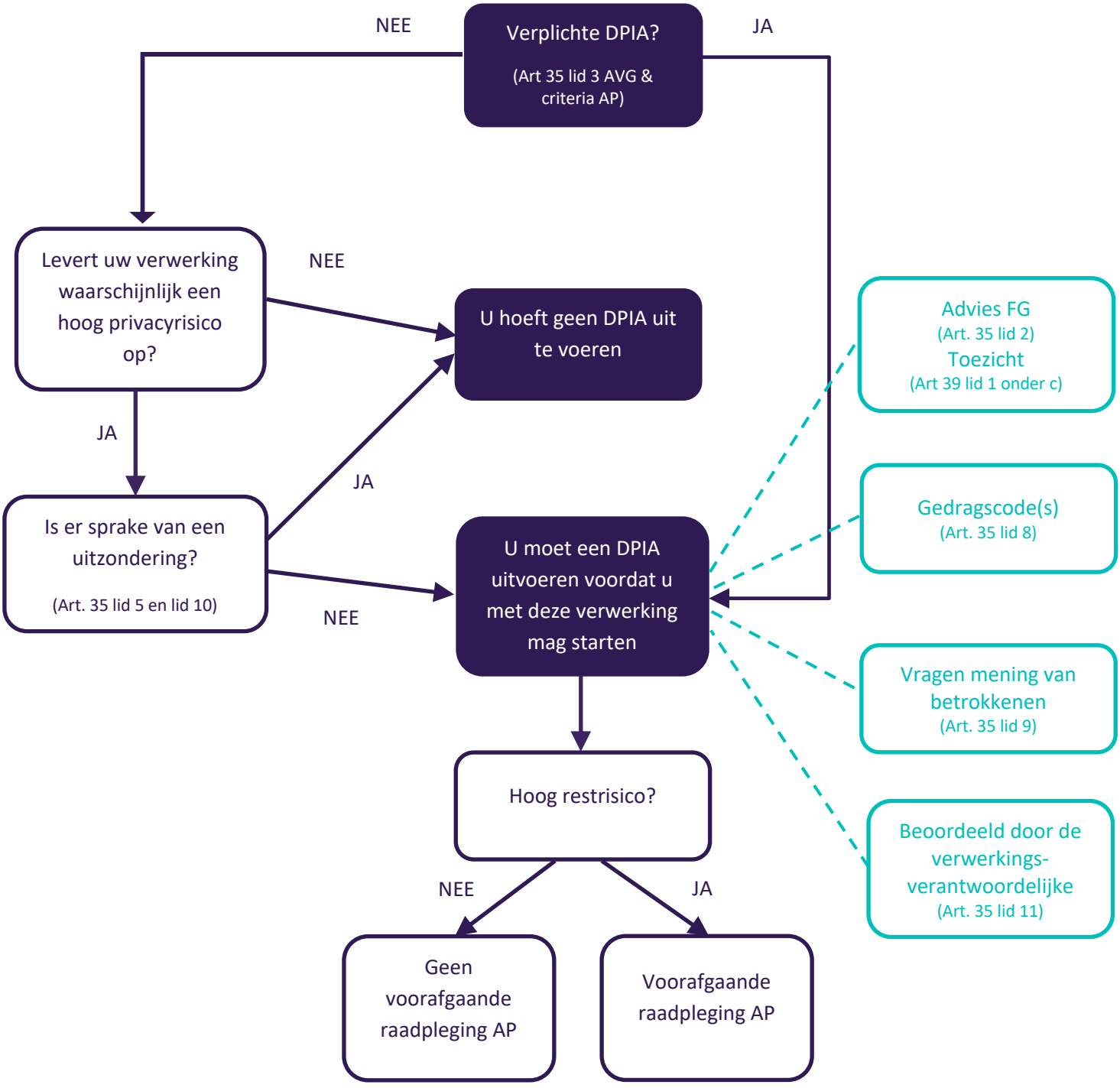
Een DPIA-proces[5] ziet er volgens de guidelines DPIA van de toenmalige Artikel 29-Werkgroep (nu European Data Protection Board ofwel EDPB) als volgt uit:



[5] In de praktijk zullen de fases, voordat de DPIA afgerond kan worden, waarschijnlijk meerdere keren worden herhaald.

BESLISBOOM

Om te bepalen of de verwerkingsverantwoordelijke een DPIA dient uit te voeren, kan onderstaande beslisboom worden doorlopen.



SLOTWOORD

De European Data Protection Board heeft richtlijnen over de uitvoering van een DPIA[6] geschreven waarin meer uitleg wordt gegeven over onder andere de verplichte situaties om een DPIA uit te voeren. Maar ook de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens, heeft een lijst gepubliceerd waaruit blijkt wanneer verplicht een DPIA moet worden uitgevoerd. In dit Cuccibook hebben wij beknopt willen weergeven wat een DPIA inhoudt, in welke gevallen deze verplicht is en hoe de uitvoering ervan het beste kan geschieden. Wij beogen hiermee een praktisch handvat te bieden om als basis te gebruiken om eigen interne DPIA-procedure te ontwikkelen en anders in ieder geval alvast aan de slag te kunnen gaan met de uitvoering van een DPIA.

Wil je meer informatie over het uitvoeren van een DPIA of wil je dat wij deze taak voor jou op ons nemen?

Neem dan contact op via info@cuccibu.nl I +31 (0) 85 303 2984.

Reduce Risk, Create Value!

[6] Artikel 29-Werkgroep, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev.01), 4 April 2017.

In een wereld die in toenemende mate digitaliseert, zorgt Cuccibu ervoor dat de onbegrensde mogelijkheden van deze wereld worden benut op een verantwoorde en veilige manier. Cuccibu helpt organisaties met vraagstukken op het vlak van informatiebeveiliging, privacy, cyber security en audit/compliance. Onze professionals op deze gebieden hebben de achtergrond en ervaring om met creatieve en heldere oplossingen iedere organisatie, groot of klein, te helpen!