# GDPR Update november 2018: Data Protection Impact Assessments (Dutch)

November 9, 2018

## AVGB-update november 2018: Gegevensbeschermingseffect- beoordelingen (DPIA's)

# Inleiding

In deze AVGB-update bespreken wij de verplichting voor organisaties om een Gegevensbeschermingseffectbeoordeling (een Data Protection Impact Assessment, **DPIA**) uit te voeren. Een DPIA is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzakelijkheid en evenredigheid daarvan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren, door deze risico's in te schatten en maatregelen te bepalen om die risico's in te perken.

De verplichting om DPIA's uit te voeren, bestond niet expliciet onder de nu ingetrokken Gegevensbeschermingsrichtlijn. Samen met de introductie van het "accountability-beginsel" wordt deze nieuwe verplichting gezien als de vervanging van het oude systeem van notificaties aan de toezichthouder. Dit notificatiesysteem bleek ineffectief en niet-kostenefficiënt.

# De verplichting om een DPIA uit te voeren

Het uitvoeren van een DPIA is niet voor iedere verwerkingsactiviteit verplicht. Een verantwoordelijke is pas verplicht om een DPIA uit te voeren indien een verwerkingsactiviteit "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen". De AVGB bevat een niet-uitputtende lijst van verwerkingsactiviteiten die waarschijnlijk een hoog risico inhouden:

i. een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
ii. grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten; of
iii. stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten (bijvoorbeeld door middel van cameratoezicht).

De richtsnoeren van de Artikel 29 Werkgroep (de **WG29**, die inmiddels is vervangen door de European Data Protection Board, de **EDPB**) over DPIA's bepalen dat een verwerkingsactiviteit in de meeste gevallen "waarschijnlijk een hoog risico inhoudt" als de verwerkingsactiviteit aan twee of meer van de volgende criteria voldoet:

1. Evaluatie of scoretoekenning, met inbegrip van profilering en voorspelling, van in het bijzonder "kenmerken met betrekking tot de beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses,

betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene".

2. Geautomatiseerde besluitvorming waaraan rechtsgevolgen zijn verbonden of die de betrokkenen anderszins wezenlijk treffen, zoals besluiten gemaakt door een geautomatiseerd systeem gebaseerd op een profiel om te bepalen of een persoon al dan niet in aanmerking komt voor een financieel product.
3. Systematische monitoring (dat wil zeggen, verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief gegevens verzameld via netwerken of via het "systematisch monitoren van een publiek toegankelijke plaats"), zoals cameratoezicht of werkplekmonitoringsystemen.
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard, zoals gezondheidsgegevens of gegevens met betrekking tot ras/etniciteit, maar ook informatie over persoonlijke politieke voorkeuren en strafrechtelijke gegevens.
5. Grootschalige gegevensverwerking (gelet op het aantal betrokkenen, de hoeveelheid gegevens, de duur van de verwerking en de geografische omvang van de verwerking). Bijvoorbeeld het 'tracken' van personen in het openbaar vervoer door middel van geolocatie.
6. Het aan elkaar koppelen of met elkaar combineren van datasets, bijvoorbeeld het koppelen of vergelijken van databases die voortkomen uit meerdere bronnen.
7. Gegevens over kwetsbare personen, zoals kinderen, werknemers, ouderen en patiënten.
8. Innovatief gebruik of innovatieve toepassing van nieuwe technologie of organisatorische oplossingen zoals het gebruik van kunstmatige intelligentie om besluiten te nemen.
9. Een verwerking die op zichzelf het gevolg heeft dat betrokkenen een recht niet meer kunnen uitoefenen, een dienst niet kunnen gebruiken of een contract niet kunnen afsluiten.

In zijn algemeenheid geldt dat aan hoe meer van deze criteria is voldaan, des te waarschijnlijker het is dat een verwerkingsactiviteit een hoog risico vormt en dat daarom het uitvoeren van een DPIA vereist is.

# DPIA-lijsten

Onder de AVGB zijn de Europese toezichthouders verplicht een lijst op te stellen en te publiceren van specifieke verwerkingsactiviteiten die in ieder geval een DPIA-vereisen. Om een indruk te geven van welke type verwerkingsactiviteiten op deze lijsten staan, hebben wij de tabel hieronder gemaakt:

| Nederland | België | Verenigd Koninkrijk |
|---|---|---|
| Grootschalige/systematische verwerking van persoonsgegevens voor heimelijk onderzoek (bijvoorbeeld door particuliere rechercheburea's) | Het gebruik van biometrische gegevens met het oog op de unieke identificatie van betrokkenen die zich in een openbare ruimte bevinden of in privéruimten die toegankelijk zijn voor het publiek | Verwerking door middel van nieuwe technologieën, of nieuwe toepassing van bestaande technologieën (inclusief kunstmatige intelligentie) |
| Zwarte lijsten (bijvoorbeeld over personen met slecht betalingsgedrag) | Het verwerken van gegevens die verzameld zijn bij derden om vervolgens in aanmerking te worden genomen bij de beslissing om een welbepaalde dienstverleningsovereenkomst met een natuurlijke persoon te weigeren of stop te zetten | Besluiten over de toegang van een individu tot een product, service, kans of voordeel die in enige mate gebaseerd zijn op automatische besluitvorming (inclusief profileren) of waarbij bijzondere categorieën van persoonsgegevens worden verwerkt |
| Grootschalige en/of systematische verwerkingen van persoonsgegevens in het kader | Het verwerken van bijzondere categorieën van persoonsgegevens die gebruikt worden voor doeleinden anders dan waarvoor deze werden | Grootschalige profilering van individuen |

| Nederland | België | Verenigd Koninkrijk |
|---|---|---|
| van fraudebestrijding (bijvoorbeeld door socialezekerheidsorganen) | verzameld, behoudens wanneer de verwerking hetzij gebaseerd is op toestemming van de betrokkene, hetzij noodzakelijk is om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke | |
| Grootschalige/systematische verwerkingen voor de beoordeling van kredietwaardigheid | Het verwerken van persoonsgegevens met behulp van een implantaat en waarbij een inbreuk op de persoonsgegevens de fysieke gezondheid van de betrokkene in het gedrang zou kunnen brengen | Het verwerken van biometrische gegevens |
| Grootschalige/systematische verwerkingen om de financiële situatie van een individu te bepalen | Grootschalige verwerking van persoonsgegevens van kwetsbare natuurlijke personen (waaronder kinderen) voor een doel anders dan waarvoor ze werden verzameld | Het verwerken van genetische gegevens anders dan door een individuele huisarts of andere zorgverlener voor het verlenen van medische zorg direct aan de betrokkene |
| Grootschalige/systematische verwerking van genetische persoonsgegevens | Grootschalige inzameling van persoonsgegevens teneinde de economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van natuurlijke personen te analyseren of te voorspellen | Het combineren, vergelijken of matchen van persoonsgegevens uit meerdere bronnen |
| Grootschalige/systematische verwerking van gegevens over de gezondheid | Systematische uitwisseling van bijzondere categorieën van persoonsgegevens of gegevens van zeer persoonlijke aard (zoals gegevens over armoede, werkloosheid, betrokkenheid van jeugdzorg of maatschappelijk werk, gegevens omtrent huishoudelijke en privé-activiteiten, locatiegegevens) tussen meerdere verantwoordelijken | Onzichtbare verwerking. Dat wil zeggen verwerking van persoonsgegevens die niet direct bij de betrokkene zijn verzameld, onder de omstandigheid dat de verantwoordelijke het voldoen aan artikel 14 (informatieverschaffing aan de betrokkene) onmogelijk acht of meent dat informeren een onevenredige inspanning vereist |
| Het delen van bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard in of door samenwerkingsverbanden | Grootschalige verwerking van gegevens die gegenereerd worden door middel van toestellen met sensoren die via het internet of via een ander medium gegevens versturen (‘Internet of Things’- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, et cetera) die dient om de economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van natuurlijke personen te analyseren of voorspellen | Verwerking waarbij de locatie of het gedrag van een individu wordt ‘getrackt’, inclusief maar niet beperkt tot de online omgeving |
| Stelselmatige en grootschalige monitoring van openbaar | Grootschalige/systematische verwerking van telefonie-, internet- of andere | Het gebruik van persoonsgegevens van kinderen |

| Nederland | België | Verenigd Koninkrijk |
|---|---|---|
| toegankelijke ruimten met behulp van camera's | communicatiegegevens, metagegevens of locatiegegevens van of herleidbaar tot natuurlijke personen (bijvoorbeeld wifi-tracking of verwerking van locatiegegevens van reizigers in het openbaar vervoer), wanneer de verwerking niet strikt noodzakelijk is voor en door de betrokkene gevraagde dienst | of andere kwetsbare personen voor marketingdoeleinden, profileren of andere automatische besluitvorming, of wanneer men voornemens is online diensten direct aan kinderen aan te bieden |
| Grootschalig/systematisch flexibel cameratoezicht (bijvoorbeeld het gebruik van dashboard camera's) | Grootschalige verwerking van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen wordt geobserveerd, verzameld, vastgelegd of beïnvloed, inclusief voor advertentiedoeleinden | Verwerkingen van dien aard dat een inbreuk op de persoonsgegevens de fysieke gezondheid of veiligheid van een persoon in gevaar kan brengen |
| Grootschalig/systematisch monitoren van werknemers | | |
| Grootschalig/systematisch verwerken van locatiegegevens | | |
| Grootschalig/systematisch verwerken van communicatiegegevens | | |
| Grootschalig/systematisch verwerken via Internet of Things-apparaten | | |
| Systematisch en uitgebreid profileren | | |
| Grootschalig observeren en beïnvloeden van gedrag | | |

Om grote inconsistenties te voorkomen die de gelijke bescherming van betrokkenen in gevaar kunnen brengen, heeft de EDPB recent (september 2018) opinies uitgebracht over deze lijsten.
Uit de opinies van de EDPB volgt onder andere dat:

- het verwerken van biometrische gegevens;
- het verwerken van genetische gegevens;
- het verwerken van locatiegegevens; of
- verwerkingen met gebruik van innovatieve technologieën;

op zichzelf niet noodzakelijkerwijs "waarschijnlijk een hoog risico opleveren". Het verwerken van dergelijke gegevens in combinatie met ten minste één ander criterium van WG29-lijst (zie onder "De verplichting om een DPIA uit te voeren") zal daarentegen wel een DPIA vereisen.

De huidige DPIA-lijsten moeten aangepast worden in overeenstemming met de opinies van de EDPB (voor zover dat nog niet is gebeurd).

# Indien een organisatie besluit om geen DPIA uit te voeren

Indien een organisatie gebaseerd op de bovenstaande factoren (de WG29-richtsnoeren en de lijsten van de toezichthouder) concludeert dat zij niet verplicht is om een DPIA uit te voeren, zal deze organisatie - met het oog op het accountability-beginsel - moeten vastleggen hoe zij tot deze conclusie is gekomen. De beslissing om geen DPIA uit te voeren moet geen eenmalige beslissing zijn, in die zin dat verantwoordelijken continu de verwerkingsactiviteiten moeten blijven evalueren om na te gaan en te signaleren of een activiteit waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van de berokkenen.

# Hoe moet een DPIA worden uitgevoerd?

In de AVGB staat niet beschreven hoe een DPIA moet worden uitgevoerd. De AVGB biedt verantwoordelijken de mogelijkheid om zelf een raamwerk te ontwerpen dat aansluit op bestaande werkwijzen op voorwaarde dat is voldaan aan de volgende minimumvereisten:

- een systematische beschrijving van de beoogde verwerkingsactiviteiten en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen van de verantwoordelijke;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingsactiviteiten in verhouding tot de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen; en
- de beoogde maatregelen om de risico's aan te pakken, en om aan te tonen dat aan de AVGB is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

De verantwoordelijke moet advies vragen aan de Functionaris voor de Gegevensbescherming (de **FG**) wanneer een DPIA wordt uitgevoerd. De FG houdt in de gaten of de DPIA in overeenstemming met de AVGB wordt uitgevoerd. Daarnaast moet de verantwoordelijke overwegen om de mening van de betrokkenen in te winnen over de voorgenomen verwerkingsactiviteiten.

# Wanneer moet een DPIA worden uitgevoerd?

Volgens de WG29 moet een DPIA worden gezien als een middel voor de besluitvorming over verwerkingsactiviteiten. Een DPIA moet daarom worden uitgevoerd vóórdat de verwerking wordt aangevangen. Het is aan te bevelen om een DPIA zo vroeg mogelijk in de ontwerp- en proof-of-concept-fase van de verwerkingsactiviteiten uit te voeren.

Daarnaast benadrukt de WG29 dat het uitvoeren van een DPIA een continu proces is en niet een eenmalige exercitie. Een DPIA moet voortdurend worden geëvalueerd en regelmatig opnieuw worden uitgevoerd. De Autoriteit Persoonsgegevens (de **AP**) suggereert bijvoorbeeld om een DPIA eens in de drie jaar opnieuw uit te voeren en de Belgische toezichthouder suggereert om een DPIA elke twee jaar opnieuw uit te voeren. Indien in de tussentijd veranderingen optreden in de verwerkingsactiviteiten, dan moet mogelijk opnieuw een DPIA worden gedaan.

De verplichting om een DPIA uit te voeren geldt ook voor bestaande verwerkingsactiviteiten.

# Raadplegen van de bevoegde toezichthouder

Indien uit een DPIA blijkt dat de verwerking een hoog risico oplevert, en de organisatie niet in staat is maatregelen te nemen om dat risico te beperken, dan moet een organisatie de bevoegde toezichthouder raadplegen. Als de toezichthouder van mening is dat de voorgenomen verwerkingsactiviteiten in strijd zijn met de AVGB, dan zal de toezichthouder binnen acht weken een schriftelijk advies verstrekken aan de verantwoordelijke. Dat advies kan inhouden dat bepaalde maatregelen dienen te worden genomen om te voldoen aan de AVGB of dat de beoogde verwerkingsactiviteiten niet mogen worden uitgevoerd. Of deze voorafgaande raadplegingen veel zullen plaatsvinden in de praktijk valt te bezien, omdat verantwoordelijken waarschijnlijk niet bereid zullen zijn om toezichthouders op de hoogte te stellen van verwerkingsactiviteiten met een hoog risico waarvoor zij geen mitigerende maatregelen kunnen vinden. Daarnaast valt de reactie van de toezichthouder te voorspellen: “een dergelijke verwerkingsactiviteit is in strijd met de AVGB, dus onthoud je ervan.”

# Praktische aanbevelingen

Organisaties moeten bepalen of zij verplicht zijn DPIA’s uit te voeren. Indien de organisatie besluit dat zij het uitvoeren van DPIA’s niet noodzakelijk acht, is het aan te bevelen om de ratio achter die beslissing goed vast te leggen zodat de organisatie kan aantonen dat dit besluit gebaseerd is op de relevante factoren. Het is belangrijk dat een verantwoordelijke doorlopend zijn verwerkingsactiviteiten monitort om te bepalen of een beslissing om geen DPIA uit te voeren wellicht heroverwogen dient te worden.

Indien een organisatie tot de conclusie komt dat zij een DPIA moet uitvoeren, dient zij ervoor te zorgen dat in ieder geval aan de minimumvereisten voor een DPIA is voldaan. Met betrekking tot uitgevoerde DPIA’s is het aan te bevelen dat een organisatie een procedure opzet om de DPIA periodiek opnieuw uit te voeren (bijvoorbeeld eens in de twee of drie jaar). In ieder geval moet een DPIA opnieuw worden uitgevoerd wanneer er veranderingen plaatsvinden in de onderliggende verwerkingsactiviteit(en).

Het is van groot belang dat organisaties intern bewustzijn creëren met betrekking tot het verwerken van persoonsgegevens en, in het bijzonder, de verplichting om DPIA’s uit te voeren. De relevante personen binnen de organisatie (bijvoorbeeld de belangrijkste personen binnen het IT-team, HR, Inkoop en Productontwikkeling) moeten bewust zijn van het DPIA-beleid van de organisatie en ook de handvatten hebben om dit uit te voeren. De FG, of een andere persoon die verantwoordelijk is voor de implementatie van de AVGB binnen de organisatie, moet verantwoordelijk zijn voor het creëren van dit bewustzijn.

Klik hier om u aan te melden voor deze nieuwsbrief.

# Overzicht behandelde onderwerpen

| | |
|---|---|
| Januari 2017 | Territoriale reikwijdte van de AVGB |
| Februari 2017 | Het concept van toestemming |
| Maart 2017 | Bijzondere persoonsgegevens |
| April 2017 | 'Accountability', 'Privacy by Design' en 'Privacy by Default' |
| Mei 2017 | Rechten van betrokkenen (informatievoorziening) |
| Juni 2017 | Rechten van betrokkenen (inzage, correctie en overdraagbaarheid) |
| Juli 2017 | Rechten van betrokkenen (wissing, beperking, bezwaar en geautomatiseerde besluitvorming) |

| | |
|---|---|
| Augustus 2017 | Verwerkers |
| September 2017 | Datalekken en meldplichten |
| Oktober 2017 | Functionaris voor de Gegevensbescherming |
| November 2017 | Doorgifte van persoonsgegevens (buiten de EER) |
| December 2017 | Toezichthouders (competenties, taken en bevoegdheden) |
| Januari 2018 | One Stop Shop |
| Februari 2018 | Sancties |
| Maart 2018 | Verwerkingen van persoonsgegevens in arbeidsverhoudingen |
| April 2018 | Profiliering en Retail |
| Mei 2018 | Overview |
| Oktober 2018 | Overzicht van ontwikkelingen sinds 25 mei 2018 |
| November 2018 | Gegevensbeschermingseffectbeoordelingen (DPIA's) |

# Your Key Contacts


**Marc Elshof**
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

**Celine van Es**
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com