Data Protection Impact Assessment uitvoeren

Het hoe en wat

BP
dELIVERY

Inleiding

Met nog minder dan 100 dagen te gaan voor de effectuering van de Algemene Verordening Gegevensbescherming (AVG) ook wel de GDPR (General Data Protection Regulation) genoemd, is er momenteel nog veel onduidelijk. Een van die zaken is de zogenaamde "2 uit 10" vuistregel en de andere onduidelijkheid betreft welke hoeveelheid data nu classificeert als "grootschalige verwerking".

Beide zaken staan echter synoniem aan de plicht tot het al dan niet uitvoeren van een "Data Protection Impact Assessment", afgekort een DPIA. Wanneer is het verplicht om een DPIA uit te voeren, wanneer niet en wat zijn de verdere verplichtingen die bij het uitvoeren van een DPIA om de hoek komen kijken. De laatste vraag die zich aandient is HOE men een DPIA uitvoert, want ook daar is nog veel onhelderheid over.

Dit whitepaper gaat in op de vele onduidelijkheden rondom de invoering van de AVG, wat er momenteel speelt en hoe men in ieder geval kan voldoen aan de wetgeving die eigenlijk al langer bestaat, maar volledig ingevoerd moet zijn op 25 mei 2018. Dit whitepaper is een verdere uitvoering van een eerder gepubliceerd whitepaper in mei 2017 en deze kunt u ook kosteloos downloaden van onze website: https://www.bpdelivery.com/nl/downloads/

Auteur

Maurice van der Woude, CEO bij BPdelivery B.V. en specialist op het gebied van security-, kwaliteit- , (cloud)ketenmanagement en ISO certificeringen.

Verantwoording

Voor de totstandkoming van dit whitepaper is de website van de autoriteit persoonsgegevens geraadpleegd en de Nederlandse vertaling van de richtsnoeren van de gegevensberschermingseffectbeoordelingen van de Werkgroep 29 (wp248_rev.01_nl)

Disclaimer

Richtsnoer

De Autoriteit Persoonsgegevens is nou niet bepaald scheutig met het geven van duidelijke en ondubbelzinnige informatie. Een van de oorzaken is gelegen in het feit dat de AVG zelf in haar oorspronkelijke vorm veel zaken niet echt duidelijk specificeert en een hoop zaken aan de markt zelf overlaat. Geen goede zaak, want als er boetes van significante hoogtes opgelegd kunnen worden, is dit voer voor juristen als er een boete wordt uitgedeeld die juridisch aangevochten kan worden. De Autoriteit Persoonsgegevens zal dan ondubbelzinnig moeten kunnen aantonen dat de uitgedeelde boete, en de hoogte daarvan, gerechtvaardigd is. Hoe dit uiteindelijk zal uitwerken is nog een beetje koffiedik kijken. De Autoriteit Persoonsgegevens was al met voorwerk bezig om een aantal "cases" te bekijken die hoofdzakelijk gingen over de doelbeperking en de duur van het bewaren van gegevens door een tweetal gerenommeerde uitzendbureaus. Deze onderzoeken werden uitgevoerd in het kader van de Wet Bescherming Persoonsgegevens (WBP) en namen 2 jaar in beslag. In 2014 werd vastgesteld dat de uitzendbranche zich onvoldoende hield aan de bepalingen in het kader van de WBP en in juli 2016 werden deze cases concreet gemaakt waarbij de beide uitzendbureaus hun interne procedures op het verzamelen en distribueren van persoonsgegevens hebben aangepast. Hierbij zijn geen boetes uitgedeeld. De Wet Bescherming Persoonsgegevens zal overigens per 25 mei 2018 vervangen worden door de AVG. De wet Datalekken van 1 januari 2016 zal een onderdeel gaan uitmaken van de AVG.

Brussel

Omdat er nog zoveel onhelder is met betrekking tot de richtsnoeren van de AVG, en dit uiteraard niet alleen voor Nederland geldt, maakt ook de (ICT) industrie zich zorgen over hoe de wet moet worden toegepast. Om hier meer duidelijkheid in te geven is in Brussel al geruime tijd een werkgroep aan de slag om een "Code of Conduct" (CoC) te ontwikkelen die in ieder geval meer duidelijkheid moet verschaffen over hoe je als organisatie nu compliant kan zijn en de torenhoge boetes kan vermijden. Deze Code of Conduct wordt momenteel nog door "Working Party 29" getoetst op compliance met de AVG. Er is op dit moment al een concept van de Code gereed maar de leden van de werkgroep weten dat deze nog niet voldoet aan de volledige set van vereisten uit de wet om tot marktpublicatie over te gaan. Leden van de CoC werkgroep mikken op de eerste releasedatum van deze code nog voor de daadwerkelijke AVG invoeringsdatum van 25 mei. Daarna is het werk zeker nog niet gedaan omdat deze code verder ontwikkeld zal worden op basis van "cases" die vanuit de markt komen en meer inzicht kunnen verschaffen in de uiteindelijke werking van de AVG zelf.

DPIA

Voor organisaties die grote hoeveelheden persoonsinformatie verwerken, kan het uitvoeren van een Data Protection Impact Assessment (DPIA) verplicht zijn. Een DPIA is een instrument om *vooraf* de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te adresseren. Zorginstellingen en rijksoverheden zijn sowiezo verplicht een DPIA uit te voeren. Maar wanneer ontstaat deze verplichting en op welke gegevensverwerkingen moeten DPIA's uitgevoerd worden? Rest ook nog de vraag hoe een DPIA er dan uit moet zien om aan de vereisten te kunnen voldoen. Even een korte opfrisser;

Er wordt als vuistregel gehanteerd dat als minstens 2 van de 10 onderstaande criteria van toepassing zijn, de organisatie verplicht is een DPIA uit te voeren[1]:

Evaluatie of scoretoekenning

Profielbepaling of voorspelling van kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene

Geautomatiseerde besluitvorming met rechtsgevolg of wezenlijk gevolg

Hieronder vallen verwerkingen die gericht zijn op het nemen van beslissingen met betrekking tot betrokkenen "waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden" of die "de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen

Stelselmatige monitoring

Verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens. Denk hierbij bijvoorbeeld ook aan cameratoezicht binnen ruimtes waarbij

[1] Bron: WP248 rev.01_nl / Guidelines DPIA

deze opnames gebruikt kunnen worden voor onder andere rechtsvervolging.

Gevoelige gegevens of gegevens van persoonlijke aard

Dit omvat speciale categorieën persoonsgegevens (bijvoorbeeld informatie over de politieke opvattingen van personen), evenals persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten maar ook medische dossiers vallen onder deze classificatie.

Grootschalige gegevensverwerkingen

Alhoewel de AVG niet expliciet definieert wat onder "grootschalig" verstaan wordt, geeft zij wel aan de volgende factoren hierbij te overwegen;

- het aantal betrokkenen binnen een relevante populatie;
- het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
- de duur, of het permanente karakter, van de gegevensverwerkings-activiteit;
- de geografische omvang van de verwerkingsactiviteit.

Matching of samenvoeging van datasets

Hierbij wordt als voorbeeld genoemd: Datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd EN die verder gaan dan de verwachting van de betrokkene.

Gegevens over kwetsbare personen

Vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke is dit criterium opgenomen. In de praktijk komt het erop neer dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Denk hierbij aan kinderen, bejaarden, geesteszieken, asielzoekers en overige groepen die, op welke wijze dan ook, zwakker in de samenleving staan.

Gebruik of toepassing van nieuwe technologieën

In de AVG wordt duidelijk gesteld dat het gebruik van een nieuwe technologie, gedefinieerd "conform het bereikte niveau van technologische kennis", aanleiding kan geven tot de noodzaak om een gegevensbeschermingseffectbeoordeling uit te voeren. Dit komt omdat het gebruik van dergelijke technologie nieuwe vormen van gegevensverzameling en -gebruik kan inhouden, mogelijk met een hoog risico voor de rechten en vrijheden van natuurlijke personen. De persoonlijke en sociale gevolgen van het gebruik van een nieuwe technologie kunnen immers onbekend zijn.

Blokkering van een recht, dienst of contract

Dit omvat verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan toe te staan, te wijzigen of te weigeren. Denk hierbij aan organisaties die vooraf screenen of zij een dienst aan een bepaald persoon willen leveren op basis van een (financieel of ander) verleden.

Doorgifte van persoonsgegevens buiten de EU

Alhoewel deze bepaling geen onderdeel uitmaakt van de standaard regels die vanuit de DPIA opgesomd worden, is dit wel degelijk een item dat in de lijst opgenomen zal moeten worden. Zoals bekend is de AVG uitsluitend van toepassing binnen de EU lidstaten. Zodra een gegevensverwerking plaatsvindt buiten de EU zal dit hoe dan ook bekend moeten zijn met een mededeling naar de betrokkene(n).

Overzicht is altijd vereist

Naast bovenstaande specifieke bepalingen moeten alle verwerkingsverantwoordelijken overeenkomstig het verantwoordings-beginsel "*een register (bijhouden) van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden*", inclusief onder meer de verwerkingsdoeleinden, een beschrijving van de gegevenscategorieën en de ontvangers van de gegevens en "indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen en moeten ze beoordelen of een hoog risico waarschijnlijk is, zelfs als zij uiteindelijk besluiten om geen gegevensbeschermingseffectbeoordeling uit te voeren. Een gegevensbeschermingseffectbeoordeling dient altijd voorafgaand aan de gegevensverwerking plaats te vinden. Met andere woorden: Een overzicht is altijd nodig voordat aan de aanleg van een verwerking begonnen gaat worden.

Wanneer niet

De Werkgroep Working Party 29 heeft ook een aantal vuistregels aangegeven wanneer het niet strikt noodzakelijk is om een DPIA uit te voeren. Hieronder staan deze vuistregels;

1. Indien de verwerking geen "*waarschijnlijk hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen*". Hier wordt echter niet aangegeven wat men onder een waarschijnlijk hoog risico verstaat;
2. Als de aard, de omvang, de context en het doel van de verwerking zeer vergelijkbaar zijn met de verwerking waarvoor al eerder een gegevensbeschermingseffectbeoordeling is uitgevoerd;
3. Als de verwerkingen vóór mei 2018 door een toezichthoudende autoriteit zijn gecontroleerd in specifieke omstandigheden die niet zijn gewijzigd;
4. Als een verwerking een rechtsgrond heeft in het Unierecht of het lidstatelijke recht, de specifieke verwerking door de wet wordt geregeld en er al een gegevensbeschermingseffectbeoordeling is uitgevoerd in het kader van de vaststelling van die rechtsgrond;
5. Als de verwerking is opgenomen in de optionele lijst (opgesteld door de toezichthoudende autoriteit) van verwerkingen waarvoor geen gegevensbeschermingseffectbeoordeling vereist is.

Om deze Europese en nationale regels te volgen, is het nagenoeg niet te doen voor kleinere bedrijven om na te gaan of zij mogelijk geen DPIA uit zouden hoeven voeren. Geadviseerd wordt dan ook om de "2 uit 10" regel te volgen om in ieder geval zeker te zijn dat aan de standaard wet wordt voldaan.

De DPIA zelf

Om vast te stellen of een gegevensverzameling aan de 2 uit 10 regel voldoet kan men volstaan met een simpel overzicht van gegevensverzamelingen waarbinnen persoonsgegevens geregistreerd worden. Zie onderstaand voorbeeld;

Applicatienaam	Verzameling	Verzameling
DPIA Onderdeel	X	Y
Beoordeling op persoonskenmerken	0	0
Geautomatiseerde beslissingen	0	0
Grootschalige persoonsmonitoring*	0	0
Gevoelige gegevens	0	1
Grootschalige gegevensverwerkingen*	0	0
Gekoppelde Databases	1	1
Gegevens over kwetsbare personen	0	0
Gebruik van nieuwe technologie	0	0
Doorgifte persoonsgegevens buiten EU	0	0
Blokkering dienst op basis kenmerken	0	0
Totalisering waarden	1	2
Aantal registraties	<nummeriek>	<nummeriek>
eventuele Koppelingen	Naam Dataset	Naam Dataset

(*) Zorg ervoor dat de term "Grootschalig" gekoppeld is aan een absoluut getal, gebaseerd op de gevoeligheid van de verwerking van die gegevens. Hier is dan vastgesteld wat de organisatie onder deze term verstaat en waarom voor dit specifieke absolute getal gekozen is.

Als blijkt dat gegevensverzamelingen aan de "2 uit 10" regel voldoen zal deze verder onderworpen moeten worden aan een gedegen onderzoek, waarbij de volgende elementen in ieder geval geadresseerd moeten worden in een gegevensbeschermingseffectbeoordeling;

Beschrijf de beoogde verwerking

Wat wordt verwerkt en welk doel wordt hiermee nagestreefd

Beoordeling

Beschrijf waarom deze verwerking plaatsvindt en welke gegevens met welk doel worden opgeslagen en/of verwerkt. Let hierbij vooral op de evenredigheid van die verwerking. Is het werkelijk noodzakelijk dat een gegeven wordt verwerkt of kan de dataset ook zonder dit gegeven functioneren binnen het doel

Beoogde maatregelen

Welke maatregelen zijn getroffen om de veiligheid van de verwerking te kunnen waarborgen en om te voldoen aan de wet en regelgeving die aan het type verwerking zijn verbonden

Beoordeling risico's

Beoordeel of de gegevensverwerkingen risico's met zich meebrengen daar waar het gaat om de rechten en vrijheden van het individu waarover binnen de dataset gegevens zijn vastgelegd

Maatregelen

Als bij de beoordeling blijkt dat er risico's zijn, geef in deze sectie dan aan welke maatregelen getroffen zijn om de risico's zoveel mogelijk te beperken. Uiteraard moeten deze maatregelen ook weer in lijn zijn met de AVG

Documentatie

Zorg dat van alle gegevensverwerkingen de documentatie op orde is. Dat houdt in dat per gegevensverzameling waarover een DPIA is uitgevoerd, registratie aanwezig is. Dit is nodig om aan te kunnen tonen welke overwegingen een rol hebben gespeeld bij de uitvoering van de DPIA en welke maatregelen per dataset genomen zijn om risico's te beoordelen en te adresseren. Ook in het kader van toetsing en evaluatie is documentatie

onontbeerlijk.

Toezicht en evaluatie

Het is niet altijd verplicht om een Functionaris gegevensbescherming aangesteld te hebben. Er moet echter wel geborgd zijn dat bij iedere uitgevoerde DPIA regelmatige evaluatie van de gegevensverwerkingen plaatsvindt en dat onafhankelijke toezicht plaatsvindt. Om dit te kunnen borgen kan gedacht worden aan jaarlijkse evaluatie door een onafhankelijke partij middels interne audits.

Bovenstaande kan samengevat worden in onderstaand model;

De AVG laat verwerkingsverantwoordelijken vrij om de exacte structuur en vorm van de gegevensbeschermingseffectbeoordeling te bepalen, zodat zij deze beoordeling kunnen laten passen bij reeds geïmplementeerde werkprocessen die, al dan niet, onderdeel uit kunnen maken van een

certificering. Ongeacht de vorm moet de beoordeling een echte risicobeoordeling zijn op basis waarvan verwerkingsverantwoordelijken maatregelen kunnen nemen om de risico's aan te pakken en te beheersen.

Publiceren of niet

Het is niet verplicht om de gegevenseffectbeoordeling te publiceren maar het wordt wel gestimuleerd om minstens delen te publiceren om het vertrouwen te vergroten bij de personen waarover gegevens verwerkt worden dat gegevens juist verwerkt worden en dat een DPIA is uitgevoerd waarbij de effecten beoordeeld zijn door, bij voorkeur, een onafhankelijke partij.

Meer Informatie

Wilt u meer informatie naar aanleiding van dit whitepaper of advies hoe u uw organisatie het beste kan voorbereiden in het kader van deze wetgeving?

Kerkstraat 85
6871 BJ, RENKUM
The Netherlands
mail: info@bpdelivery.com
web: www.bpdelivery.com

Over BPdelivery

BPdelivery richt zich op de optimalisatie van geautomatiseerde bedrijfsprocessen tussen service-, ICT- en facility organisaties, hun interne gebruikers en externe leveranciers. Daarnaast wordt BPdelivery veel gevraagd voor adviestrajecten op Informatiebeveiliging, kwaliteits-management, NEN7510, SOC/ISAE en overige organisatie vraagstukken van strategische aard.