INFORMATIE
BEVEILIGINGS
DIENST

Handleiding

Checklist Data Privacy Impact Analyse

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Checklist Data Privacy Impact Analyse

Versienummer
1.1

Versiedatum
09-08-2018

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Copyright

Rechten en vrijwaring
De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
0.2	19-03-2018	Versie ter interne review
0.5	04-06-2018	Reviewcommentaar verwerkt
1.0	13-06-2018	Versie gereed voor publicatie
1.1	09-08-2018	Lijst van AP met verwerkingen opgenomen waarvoor DPIA verplicht is.

INFORMATIE
BEVEILIGINGS
DIENST

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

VNG
Realisatie

1. Inleiding

Gemeenten zitten regelmatig met de vraag voor welke verwerkingen een data protection impact assessment (DPIA) uitgevoerd moet worden en wanneer. In artikel 35 (Gegevensbeschermingseffectbeoordeling) van de AVG staat beschreven wanneer een DPIA uitgevoerd moet worden. Om meer duiding aan de eisen uit artikel 35 te geven heeft de werkgroep van Europese privacytoezichthouders (WP29) aanvullende kaders opgesteld die ook op de site van de Autoriteit Persoonsgegevens (AP) gepubliceerd staan[1].

Onderstaande checklist is van deze kaders afgeleid en dient als handreiking om te bepalen wanneer het verplicht is een DPIA uit te voeren:

1.1. Uitgangspunten

De AP heeft een lijst van soorten verwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is vóórdat u met verwerken begint.[2] De lijst, met 16 specifieke verwerkingen, is niet uitputtend. Het kan zijn dat uw verwerking niet op deze lijst staat. In dat geval moet u beoordelen of uw verwerking een hoog privacyrisico oplevert voor de betrokkenen.
U hoeft waarschijnlijk geen DPIA uit te voeren wanneer uw gegevensverwerking:

- Waarschijnlijk geen hoog privacyrisico oplevert.
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de AP oordeelt dat er toch een DPIA nodig is.
- Op een lijst[3] staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de AP de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht.

Mocht een gegevensverwerking niet op de lijst van de AP met verwerkingen voorkomen waarvoor een DPIA verplicht is en aan een van de bovenstaande punten voldoen is het toch raadzaam de onderstaande vragen even na te lopen om te bepalen of het niet toch beter is een DPIA uit te voeren.

1.2. Checklist

Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als een verwerking niet voldoet aan bovenstaande uitzonderingen en als op 2 of meer van de onderstaande vragen positief geantwoord kan worden:

1. De verwerking dient ter beoordeling van mensen op basis van persoonskenmerken:

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. Voorbeelden hiervan zijn lijstjes van mensen in belangengroepen, verenigingen etc. waaruit persoonlijke voorkeuren en of interesses af te leiden zijn, het profileren van hangjongeren op basis van facebook (gedrag) of wifi-tracking (locatie of verplaatsingen).

2. De verwerkte gegevens worden gebruikt voor geautomatiseerde beslissingen:

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd. Dit zou bijvoorbeeld kunnen spelen bij geautomatiseerd besluiten of iemand wel of niet recht heeft op een uitkering of een Wmo-voorziening.

3. De gegevens worden gebruikt voor stelselmatige en grootschalige monitoring:

---

[1] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

[2] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667

[3] Het zou kunnen zijn dat de DPIA niet nodig is omdat de AP gebruik gemaakt heeft van artikel 35 lid 5 (de verwerking staat op een lijst waarvan door de AP is vastgesteld dat geen DPIA nodig is).

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht (art 151c Gemeentewet).

4. De verwerking bevat gevoelige gegevens:
Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG). Hierbij moet je denken aan het vastleggen van gegevens over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, het lidmaatschap van een vakbond, genetische en biometrische gegevens, gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Daarnaast moet het BSN ook als bijzonder persoonsgegeven beschouwd worden aangezien deze alleen gebruikt mag worden als dit bij wet is voorgeschreven.

5. De verwerking betreft een grootschalige gegevensverwerking:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming#wat-ziet-de-avg-als-een-grootschalige-verwerking-van-persoonsgegevens-6019

6. Gekoppelde databases:
Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn (zoals bijvoorbeeld bij Suwi).

7. De verwerking bevat gegevens over kwetsbare personen:
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 niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Kwetsbare personen zijn onder andere kinderen jonger dan 16 jaar, mensen in de schuldhulp of personen die aanspraak maken op de Wmo.

8. De verwerking maakt gebruik van nieuwe technologieën:
De AVG is er duidelijk over dat een PIA 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.

9. Bij de verwerking vindt doorgifte van persoonsgegevens buiten de EER plaats:
De bescherming van persoonsgegevens is niet in alle landen hetzelfde geregeld. Buiten de EER is het daarom niet zeker dat een land voldoende bescherming biedt. Voor een aantal landen buiten de EER heeft de EU bepaald dat deze een vergelijkbaar beschermingsniveau van privacy bieden als binnen de EER[4]. Voor doorgifte naar de VS geldt dat het beschermingsniveau alleen als adequaat beschouwd wordt als deze verwerking binnen het privacy shield[5] plaats vindt.

10. De verwerking kan mogelijk leiden tot de blokkering van een recht, dienst of contract van betrokkenen:
Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen een recht (zoals het recht op een uitkering of een Wmo voorziening) niet kunnen uitoefenen, dat zij een dienst niet kunnen gebruiken of dat zij een contract niet kunnen afsluiten.

2. Moment van uitvoeren

Start met het uitvoeren van de DPIA zo vroeg als praktisch gezien mogelijk is in de ontwerpfase van de gegevensverwerking. Ook als nog niet alle details van de verwerking bekend zijn. Door vroeg te beginnen, is het voor u makkelijker om aan de wettelijk vereiste principes van privacy by design en privacy by default te voldoen.

[4] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
[5] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

Continu proces

Let op: dat u de DPIA misschien gaandeweg moet aanpassen, is geen argument om de DPIA uit te stellen of achterwege te laten. Een DPIA uitvoeren is geen eenmalige opdracht, maar een continu proces. U zult altijd moeten (blijven) monitoren of uw gegevensverwerking wijzigt en of u daarom de DPIA moet bijstellen.

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl