Data Protection Impact Assessment (DPIA)

Gegevensbeschermingseffectbeoordeling

Template door Sieuwert van Otterloo [www.softwarezaken.nl](http://www.softwarezaken.nl)

U moet het eerste deel van dit template invullen voor alle gegevensverwerkingen. Hiermee legt u waarom er wel of niet een DPIA moet worden uitgevoerd.

Bronnen template

Dit template is ontwikkeld op basis van de volgende bronnen:

* De AVG zelf
* De Handleiding Algemene Verordening Gegevensbescherming, uitgave van de Autoriteit Persoonsgegevens. Auteurs: Bart W. Schermer, Dominique Hagenauw, Nathalie Falot
* Richtsnoeren voor gegevensbeschermingseffectbeoordelingen door groep Gegevensbescherming, Zoals laatstelijk gewijzigd en vastgesteld op 4 oktober 2017
* Privacy Impact Assessment (PIA): Introductie, handreiking en vragenlijst Versie 1.2 - November 2015 uitgegeven door NOREA

# Organisatiegegevens

Naam, adres van organisatie:

Opsteller DPIA:

Naam en contactgegevens FG (als deze is aangesteld):

Overige betrokkenen en geraadpleegde experts:

Stappenplan uitvoering:

Geef hier aan op welke dag er met wie is gesproken, of op welke dag er workshops zijn geweest en welke partijen/personen hierbij aanwezig waren.

# Gegevens van de verwerking

Beschrijf hier om welke persoonsgegevens het gaat (naam, email, medisch, …).

Met welk doel en in welk proces worden deze gegevens gebruikt?

Welke groepen betrokkenen zijn de persoonsgegevens van (websitebezoekers, leerlingen, klanten, …)

Is deze DPIA voor een bestaande situatie, of voor een nieuw voorgestelde situatie?

# Moet een DPIA worden uitgevoerd

Een DPIA is verplicht als de gegevensverwerking voorkomt op de volgende lijst met onderwerpen die door de Autoriteit Persoonsgegevens is gepubliceerd:

1. Heimelijk toezicht
2. Zwarte lijsten
3. Fraudebestrijding
4. Creditscores
5. Financiële situatie
6. Genetische persoonsgegevens
7. Gezondheidsgegevens
8. Samenwerkingsverbanden
9. Cameratoezicht
10. Flexibel cameratoezicht
11. Controle werknemers
12. Locatiegegevens
13. Communicatiegegevens
14. Internet of things
15. Profilering
16. Observatie en beïnvloeding van gedrag
17. Biometrische gegevens

Verder is een DPIA verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo als een organisatie:

1. systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering;
2. op grote schaal bijzondere persoonsgegevens verwerkt;
3. op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Om te bepalen of er mogelijk sprake is van een hoog risico hanteren de toezichthouders de onderstaande vuistregel. Er is sprake van een hoog risico men aan twee of meer van de onderstaande negen criteria voldoet:

1. evaluatie van personen of scoretoekenning;
2. geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
3. stelselmatige monitoring;
4. gevoelige gegevens of gegevens van zeer persoonlijke aard;
5. op grote schaal verwerkte gegevens;
6. matching of samenvoeging van datasets;
7. gegevens met betrekking tot kwetsbare betrokkenen;
8. innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
9. blokkering van een recht, dienst of contract.

Aan welke criteria voldoet deze verwerking? Geef voor elk criteria een korte motivatie

# Systematische omschrijving van de gegevensverwerking

Beschrijf hier in meer detail hoe de gegevensverwerking gaat.

Hoe / waar wordt de informatie verzameld?

Waar wordt deze opgeslagen? Wie kan hier bij?

Hoe wordt de informatie gebruikt? Wordt elk veld gebruikt?

Wat zijn de doelen van de verwerking? Kunnen deze doelen ook zonder de gegevens worden behaald?

Wordt binnen het proces om toestemming gevraagd? Zijn er latere uitschrijf/opt-out-mogelijkheden?

Wat is de bewaartermijn van de gegevens? Hoe is de verwijdering van de gegevens geregeld?

Welke hardware en software wordt gebruikt bij de gegevensverwerking?

Welke afdelingen, leveranciers en andere partijen zijn als verwerker bij de verwerking betrokken?

Is er sprake van internationale doorgifte? Welke landen betreft dit?

Waar wordt de data gearchiveerd? Is dit papier of digitaal?

Wat is de verwachte omvang van de gegevensverwerking (aantallen betrokkenen)

# Beoordeling noodzaak en proportionaliteit

Is er sprake van een duidelijk gespecificeerd doel? Wat is dit doel precies, en waarom is dit legitiem?

Kan dit doel ook zonder deze persoonsgegevens worden behaald? Waarom niet, of waarom doet u het niet anders?

Is er sprake van een duidelijke maximale bewaartermijn?

Wordt er voldoende informatie verstrekt aan betrokkene? Is het voor betrokkenen duidelijk welke rechten zij hebben en hoe zij deze kunnen uitoefenen?

Hoe is het recht op inzage gewaarborgd?

Hoe is het recht op rectificatie gewaarborgd?

Hoe is het recht op verwijdering gewaarborgd?

Hoe is het recht op overdraagbaarheid van gegevens gewaarborgd?

# Beoordeling van de privacyrisico's

## Inschatting risico’s

Hoe schat u de kans en impact van de volgende risico’s:

|  |  |  |  |
| --- | --- | --- | --- |
| Risico | Hoe kan dit risico zich voordoen? | Kans dat dit in een jaar gebeurt | Impact op betrokkenen |
| Onrechtmatige toegang – interne medewerkers |  | Hoog want.. | Laag want… |
| Onrechtmatige toegang – door buitenstaanders |  |  |  |
| Ongewenste wijziging van gegevens – interne medewerkers |  |  |  |
| Ongewenste wijziging van gegevens – door buitenstaanders |  |  |  |
| Verdwijnen / zoekraken van gegevens |  |  |  |

Wat is de exacte impact van uitlekken van gegevens op betrokkenen?

* Heeft dit nadelige gevolgen voor de persoon?
* Is er kans op financiële schade?
* Is er kans op identiteitsdiefstal of fraude?

# Maatregelen

Kunt u per risico aangeven welke maatregelen u neemt om de gegevens te beschermen:

Zijn er nog aanvullende organisatorische maatregelen die u neemt?

Zijn er nog aanvullende technische maatregelen die u neemt?

Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen? Wie is dit:

# Advies van de FG

Heeft u een Functionaris voor de Gegevensbescherming (FG) benoemd? Dan is het verplicht om deze persoon om advies te vragen. Leg het advies van de FG hieronder vast:

Naam FG:

Datum van advies:

Antwoorden van FG:

Zijn de gegevensverwerking en doeleinden duidelijk omschreven?

Is er de verwerking van de persoonsgegevens noodzakelijk of proportioneel voor de doeleinden?

Zijn de privacyrisico’s voldoende in kaart gebracht? Welke risico’s ontbreken nog?

# Advies van betrokkenen en vertegenwoordigers

Is er voor deze DPIA gesproken met betrokkenen of vertegenwoordigers? Welke reactie hebben zij gegeven? Hoe is deze reactie verwerkt?

# Voorafgaande raadpleging

Komt er uit de DPIA dat de verwerking een hoog risico oplevert als u geen risicobeperkende maatregelen neemt? Geef antwoord en motivatie hieronder:

…

Indien ja, dan moet u een voorafgaande raadpleging aanvragen bij de Autoriteit Persoonsgegevens (AP). Hierbij moet u de DPIA aan de AP verstrekken.

## Appendix Toetsvragen impact NOREA

*Het gebruik van deze appendix is optioneel, ter verbetering van de beoordeling privacy-risico’s. Nieuwe inzichten uit deze vragen moet u in het hoofddocument verwerken. We raden aan om deze vragen ook te beantwoorden, om zo de gegevens inschattingen hierboven te toetsen. De vragen komen uit de NOREA handreiking.*

Bij ja-antwoorden op deze vragen geldt: U loopt verhoogde risico’s, de impact van uw project op de betrokkenen en de wijze waarop deze gaan reageren is moeilijk in te schatten. Dit kan leiden tot verhoogde kans op imagoschade, verstoring van de bedrijfscontinuïteit, en acties door handhavers en toezichthouders.

Is er sprake van invoering van nieuwe technologie? Bijvoorbeeld intelligente transportsystemen, locatie of volgsystemen op basis van GPS, mobiele technologie, gezichtsherkenning in samenhang met cameratoezicht.

Is er sprake van invoering van technologie die bij het publiek vragen of weerstand op kan roepen? Bijvoorbeeld biometrie, RFID, behavioural targeting (profilering).

Is er sprake van invoering van bestaande technologie in een nieuwe context? Zoals cameratoezicht of drugscontrole op de werkvloer.

Is er sprake van andere grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt? Bijvoorbeeld het samenvoegen of koppelen van verschillende overheidsregistraties, invoering van nieuwe vormen van identificatie of vervanging van een systeem waarin persoonsgegevens worden opgeslagen.

Is er (naast de AVG) veel wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft? Houd bij de beantwoording rekening met: 1. Sectorale wetgeving. 2. Gedragscodes. 3. Algemene maatregelen van bestuur. 4. Jurisprudentie. 5. Internationale aspecten.

Zijn er veel maatschappelijke belanghebbenden? Denk aan Medewerkers, afnemers, leveranciers, belangengroeperingen, burgers, klanten toezichthouders. Welke beroepsgroepen betrokken zijn bij de verwerking?

Zijn er bij veel partijen betrokken de uitvoering van het project? Houd bij de beantwoording rekening met: 1. Aannemers en dienstverleners. 2. Hardware- en softwareleveranciers. 3. IT Service Providers.

Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?

Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)? Denk hierbij bijvoorbeeld ook aan geolocatie, personeelsvolgsystemen, beslisondersteuning bij het als dan niet aanbieden van producten of diensten.

Verwerkt u bijzondere persoonsgegevens, gevoelige persoonsgegevens, unieke biometrische kenmerken, BSN-nummers of andere gegevens waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid? Bijvoorbeeld vingerafdrukken, DNA-profielen, creditcardinformatie, financiële informatie, erfrechtelijke aspecten, arbeidsprestaties of gegevens waarvoor een geheimhoudingsplicht geldt?

Verwerkt u gegevens over kwetsbare groepen of personen? Bijvoorbeeld minderjarige personen, verstandelijk gehandicapten, gedetineerden, onder toezicht gestelden, mensen van wie de fysieke veiligheid in gevaar is.

Hebben de gegevens betrekking op de gehele of grote delen van de bevolking van een land?

Worden de gegevens verkocht aan derde partijen?

## Bijlage 2 – Criteria voor een aanvaardbare gegevensbeschermingseffectbeoordeling

De Europese werkgroep Groep Gegevensbescherming artikel 29 (afgekort WP29) heeft een document gepubliceerd *‘Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679’*.

Hierin staat een lijst criteria die u kunt gebruiken om te beoordelen of een gegevensbeschermingseffectbeoordeling, of een methode voor het uitvoeren van een gegevensbeschermingseffectbeoordeling, volledig genoeg is om aan de AVG te voldoen.

**Er wordt een systematische beschrijving van de verwerking verstrekt (artikel 35, lid 7, onder a)):**

* er wordt rekening gehouden met de aard, omvang, context en doelen van de verwerking (overweging 90);
* de persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden bewaard worden geregistreerd;
* er wordt een functionele beschrijving van de verwerking verstrekt;
* de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen) worden geïdentificeerd;
* er wordt rekening gehouden met de naleving van de goedgekeurde gedragscodes (artikel 35, lid 8);

**De noodzaak en evenredigheid worden beoordeeld (artikel 35, lid 7, onder b)):**

De beoogde maatregelen om aan de verordening te voldoen worden bepaald (artikel 35, lid 7, onder d), en overweging 90), waarbij rekening wordt gehouden met:

* maatregelen die bijdragen aan de evenredigheid en noodzaak van de verwerking op basis van:
	+ een of meer gespecificeerde, expliciete en legitieme doeleinden (artikel 5, lid 1, onder b));
	+ rechtmatigheid van de verwerking (artikel 6);
	+ toereikend, ter zake dienend en beperkt tot wat noodzakelijke gegevens zijn (artikel 5, lid 1, onder c));
	+ beperkte bewaartermijn (artikel 5, lid 1, onder e));
* maatregelen die bijdragen aan de rechten van de betrokkenen:
	+ informatie verstrekt aan de betrokkene (artikelen 12, 13 en 14);
	+ recht van inzage en recht op overdraagbaarheid van gegevens (artikelen 15 en 20);
	+ recht op rectificatie en recht op gegevenswissing (artikelen 16, 17 en 19);
	+ recht van bezwaar en recht op beperking van de verwerking (artikelen 18, 19 en 21);
	+ relaties met verwerkers (artikel 28);
	+ waarborgen omtrent internationale doorgifte(n) (hoofdstuk V);
	+ voorafgaande raadpleging (artikel 36).

**De risico's voor de rechten en vrijheden van betrokkenen worden beheerd (artikel 35, lid 7, onder c)):**

* er wordt rekening gehouden met de oorsprong, de aard, het specifieke karakter en de ernst van de risico's (zie overweging 84) of, meer specifiek, voor elk risico (onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens) vanuit het perspectief van de betrokkenen:
	+ er wordt rekening gehouden met de bronnen van de risico's (overweging 90);
	+ de mogelijke gevolgen voor de rechten en vrijheden van de betrokkenen worden geïdentificeerd in geval van gebeurtenissen zoals onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens;
	+ bedreigingen die kunnen leiden tot onrechtmatige toegang, ongewenste wijziging en de verdwijning van gegevens worden geïdentificeerd;
	+ de waarschijnlijkheid en ernst worden ingeschat (overweging 90)
* de beoogde maatregelen om de risico's aan te pakken worden bepaald (artikel 35, lid 7, onder d), en overweging 90);

**De belanghebbenden worden betrokken:**

* het advies van de functionaris voor gegevensbescherming wordt ingewonnen (artikel 35, lid 2);
* indien nodig wordt de betrokkenen of hun vertegenwoordigers naar hun mening gevraagd (artikel 35, lid 9).