

Project [.....]

Data Protection Impact Assessment

Kenmerken Data Protection Impact Assessment

Identificatienummer DPIA	[dit vult de Functionaris Gegevensbescherming in]
Naam van de verwerking	
Hoofduitvoerder PIA	
Betrokken belanghebbenden:	
Eigenaar verwerking:	Naam: Handtekening voor akkoord: Datum:
Uitgevoerd van/tot	
Revisiedatum	Max 2 jaar

Samenvatting

Inhoudsopgave

1.	Inleiding.....	4
2.	Onderkende risico's	4
3.	Advies.....	4
4.	Vragenlijst	5

1. Inleiding

2. Beschrijving systeem

[Beschrijf:

- Doel van het systeem
- Bedrijfsproces(sen) dat het systeem zal ondersteunen of ondersteunt
- Functionele eisen op hoofdlijnen
- Indien van toepassing: het kunnen voorkomen van koppelen van gegevens, transparantie, mogelijkheid voor betrokkenen en beheerders om in te grijpen
- Gegevensmodel/Gegevensstromen
- De manier waarop gegevens worden verzameld, bij wie en waarom. Tevens de grondslag van de verzameling
- Wie hebben toegang hebben tot welke gegevens onder welke omstandigheden.
- Indien van toepassing welke gegevens met welke partijen worden uitgewisseld en met welk doel
- Een verklaring ten aanzien van de rechtvaardiging van het verwerken van persoonsgegevens in kwestie] (bijv toestemming niet mogelijk)
- Gebruikersbeheer
- Housing/hosting
- Gegevensbewaring – en vernietiging.

3. Onderkende risico's

Op basis van de antwoorden op de vragen zijn de volgende privacy-risico's geïdentificeerd.

1. Verwerking;
Risico:

4. Advies

Op basis van de onderkende risico's wordt geadviseerd de standaard privacymaatregelen/ beveiligingsmaatregelen te treffen.

5. Vragenlijst

Onderstaande vragenlijst is gebaseerd op het document Privacy Impact Assessment (PIA) – introductie, handreiking en vragenlijst, versie 1.1 Juli 2015 van NOREA, de beroepsorganisatie van IT-auditors in Nederland. Bij het invullen van de vragenlijst wordt geadviseerd gebruik te maken van deze handreiking van de NOREA (zie <http://www.norea.nl>).

#	Vraag	Ja	Nee	Opmerking
1	Het type project			
1.1	Is er sprake van het verwerken van persoonsgegevens?			
1.2	Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?			
1.3	Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt uw organisatie op als verwerker?			
1.4	Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?			
1.5	Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?			
1.6	Is er sprake van:			
a	Gebruik van nieuwe technologie?			
b	Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?			
c	De invoering van bestaande technologie in nieuwe context?			
d	(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?			
e	Een nieuwe verwerking van persoonsgegevens?			
f	Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen?			
g	Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.			
1.7	Heeft u op alle bovenstaande (a t/m g) nee geantwoord?			Indien alle vragen met nee zijn beantwoord, wordt het project beschouwd als laag risico. Verdere invulling van deze DPIA vragenlijst heeft geen toegevoegde waarde

#	Vraag	Ja	Nee	Opmerking
1.8	Is er (naast de AVG) andere wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?			
1.9	Zijn er veel maatschappelijke belanghebbenden?			
1.10	Zijn er veel partijen betrokken bij de uitvoering van het project?			
1.11	Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?			
2	De gegevens			
2.1	Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?			
2.2	Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?			
2.3	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)?			
2.4	Is sprake van het verwerken van:			
a	Bijzondere persoonsgegevens?			
b	Uniek identificerende gegevens?			
c	Wettelijk voorgeschreven persoonsnummers?			
d	Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?			
2.4.1	Bij een van bovenstaande Ja: Kan het doel met andere gegevens worden bereikt die een verminderd risico op misbruik met zich mee brengen?			
2.5	Verwerkt u gegevens over kwetsbare groepen of personen?			
2.6	Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?			
3	Betrokken partijen			
3.1	Zijn er (na afronding van het project) bij het verzamelen en			

#	Vraag	Ja	Nee	Opmerking
	verder verwerken van de gegevens meerdere <i>interne</i> partijen betrokken?			
3.2	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere <i>externe</i> partijen betrokken?			
3.3	Zijn er partijen betrokken (in het project of bij de verwerking) die zich niet aan een met Nederland vergelijkbare privacywetgeving hoeven te houden?			
3.4	Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?			
3.5	Worden de gegevens verkocht aan de derde partijen?			
4	Verzamelen van gegevens			
4.1	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig?			
4.2	Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?			
4.3	Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?			
4.4	Is duidelijk of u de gegevens verzamelt op basis van opt-in (verzameling uitsluitend als de betrokkene daarvoor toestemming heeft gegeven) of op basis van opt-out (verzameling tenzij de betrokkene daartegen bezwaar heeft gemaakt)?			
4.4.1	Indien u toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken?			
4.4.2	Is de impact van het intrekken van de toestemming groot voor de betrokkene?			
4.5	Vertelt u aan de betrokkene dat de gegevens worden verzameld?			
4.5.1	Bij Nee: Kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens?			
4.5.2	Bij Ja (op vraag 4.5): Vertelt u			

#	Vraag	Ja	Nee	Opmerking
	de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?			
4.5.3	Bij Ja: (op vraag 4.5): Vertelt u de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?			
4.6	Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?			
5	Gebruik van gegevens			
5.1	Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?			
5.2	Worden gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?			
5.2.1	Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?			
5.3	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?			
5.4	Worden op basis van de gegevens beslissingen genomen over de betrokkenen?			
5.4.1	Bij Ja: leveren de gegevens een volledig en actueel beeld van de betrokkenen op?			
5.5	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?			
5.6	Worden gegevens breed verspreid binnen de organisatie?			
5.7	Worden gegevens breed verspreid buiten de organisatie?			
5.7.1	Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van de betrokkene?			
5.8	Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?			
5.8.1	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?			
5.9	Kunnen de betrokkenen hun gegevens inzien of daarom			

#	Vraag	Ja	Nee	Opmerking
	vragen?			
5.10	Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?			
5.11	Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?			
6	Bewaren en vernietigen			
6.1	Is een bewaartermijn voor de gegevens vastgesteld?			
6.2	Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?			
6.2.1	Zo ja, worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?			
7	Beveiliging			
7.1	Is sprake van intern geformuleerd beleid over het beveiligen van informatie?			
7.2	Zo ja, is duidelijk op welke wijze het project er voor zorg draagt dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?			
7.3	Zo ja, is bij het vaststellen van de maatregelen in voldoende mate rekening gehouden met de Richtsnoeren Beveiliging van persoonsgegevens die de Autoriteit persoonsgegevens heeft gepubliceerd alsmede met algemeen geaccepteerde beveiligingsstandaarden?			
8	Meldplicht datalekken			
8.1	Zijn maatregelen getroffen om datalekken te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen van wie de gegevens zijn gelekt?			
8.2	Zo ja, is bij het vaststellen van de maatregelen in voldoende mate rekening gehouden met de Richtsnoeren die de Autoriteit persoonsgegevens over de meldplicht datalekken heeft gepubliceerd			