



titel

ondertitel

Samenvatting
Data Protection Impact Assessment

Over deze risicoanalyse

Een DPIA bestaat uit het doorlichten van de verwerking om inzichtelijk te maken of de verwerking rechtmatig is, welke risico's ermee gepaard gaan en hoe je die kunt verkleinen.

Deze DPIA gaat over [variabele]. Het doel is [variabele].

De BIV-codering voor [variabele] scoort [variabele]. De betrokken persoonsgegevens vallen in een [variabele] risicoklasse, namelijk label [variabele]. Het gaat echter om veel betrokkenen. Een DPIA(-light?) is daarom vereist.

Het verwerken van persoonsgegevens vindt plaats via [variabele].

1

Deze DPIA gaat over

[variabele]

2

Doel

[variabele]

3

In opdracht van

[variabele]

4

Referenties

Verwerkingnummer: [variabele] | Ticketnummer: [variabele]

5

Aanspreekpunt

Deze DPIA is uitgevoerd door [variabele] en is voorzien van een advies door [variabele] (FG). Datum: [variabele]

Samenvatting risico's en maatregelen

Samenvatting

- Het proces waarbinnen de persoonsgegevens worden verwerkt, ...
- Risicoklasse is
- Conclusie is (rechtmatig, ... implementatie mogelijk als ...)
- De mitigerende veiligheidsmaatregelen, waarborgen en mechanismen garanderen Het de informatiebeveiliging voldoende (of: er moeten aanvullende mitigerende maatregelen worden genomen om de informatiebeveiliging en privacy voldoende te borgen.)

Risico's

- 1 **onderwerp** – toelichting risico
- 2 **onderwerp** – toelichting risico
- 3 **onderwerp** – toelichting risico



Maatregelen

- 1 **kern van de maatregel**- toelichting maatregel
- 2 **kern van de maatregel**- toelichting maatregel
- 3 **kern van de maatregel**- toelichting maatregel

Inventarisatie verwerking persoonsgegevens



Vraagstelling	Beschrijving verwerking
Wat is de behoefte/doel?	
Welke activiteiten/processen vinden daarvoor plaats?	
Welke persoonsgegevens zijn nodig?	
Over wie en om hoeveel personen gaat het?	
Manier van verzamelen	
Wie is betrokken bij het verzamelen/ opslaan en wat is de juridische verhouding?	
Welke bewaartermijn is van toepassing?	
Gaat het om een verwerking waarop een verwijderverzoek kan worden uitgevoerd?	
Is het een pilot?	
Gaat het om schaduw-IT?	
Moet de OR en/of SR worden geïnformeerd/betrokken?	

Rechtmatigheid



Een verwerking van persoonsgegevens mag alleen plaatsvinden als de verwerking de rechtmatig is en voldoet aan specifieke voorwaarden.

Voorwaarde	Voorwaarde	Antwoord (ja/nee en uitleg)
Rechtmatige verwerkingsgrondslag	De beoogde verwerking is rechtmatig/legitiem volgens de AVG	
Doelbinding	De gegevens worden alleen voor het verzameldoel gebruikt	
Dataminimalisatie	Er worden niet meer gegevens verzameld dan nodig zijn om het doel te bereiken en als ze niet meer nodig zijn, worden ze verwijderd	
Transparantie	De betrokkenen kunnen nagaan waarvoor hun gegevens worden gebruikt en zijn geïnformeerd over hun rechten	
Data-integriteit	De gegevens zijn juist en correct	
Gegevensbescherming	De gegevensbescherming voldoet aan Privacy by Design.	
Proportionaliteit Doeltreffendheid Subsidiariteit	Met de verwerking van de gegevens wordt het gestelde doel, behaald, daarover is geen onzekerheid	
	Het legitieme doel stat in verhouding tot het feit dat hiervoor persoonsgegevens moeten worden verwerkt	
	Dit de beste manier om het doel te bereiken: het doel kan niet op een andere, minder ingrijpende wijze worden bereikt	

Framework Privacy by Design

kies:  

- 1 **Anonimiseren** – Anonimiseren is ongewenst; dreiging moet te achterhalen zijn tot de bron. 
- 2 **Dataminimalisatie** – Er is sprake van dataminimalisatie? Er worden niet meer gegevens verzameld dan nodig is; de set is beperkt. 
- 3 **Pseudonimiseren** – Toelichting 
- 4 **Encryptie** – Encryptie wordt toegepast tijdens transport en tijdens opslag/in ruste. Men volgt Secure Software Design van OWASP. 

- 5 **Rechten gefaciliteerd** – Dit is in orde. Betrokkenen kunnen hun rechten uitoefenen en kunnen weten dat de ICT-voorzieningen worden gemonitord. 
- 6 **Toegangsmanagement** – De toegang is 
- 7 **Bewaren en vernietigen** – In orde. Toelichting ... 
- 8 **Veilige verwerking (en beheer)** – Privacy by Design is toegepast. 