

Handreiking Pre-scan DPIA

Versie 1.0

Datum 23 November 2023
Status Definitieve versie

Inhoudsopgave

1	Inleiding.....	3
2	Vragenlijst.....	4
	A. Inleiding / algemeen.....	4
	B. Gegevensverwerking	4
	C. Internationale doorgiften	5
	D. Lijst AP.....	5
	E. Lijst EDPB.....	6
	F. Overige	7
	G. Berekening.....	7
3	Informatie verwerkingsregister	7
4	Risico(berekening).....	8

1 Inleiding

Voorafgaand aan een verwerking van persoonsgegevens kan een organisatie op grond van de Algemene Verordening Gegevensbescherming (AVG) verplicht worden om een Gegevensbeschermingseffectbeoordeling (GEB) uit te voeren. In de Europese wetgeving wordt de GEB een Data Protection Impact Assessment (DPIA) genoemd. Binnen de Rijksoverheid wordt voor de uitvoering van een DPIA gebruik gemaakt van het Model DPIA Rijksdienst.¹ Aan de hand van de Pre-scan DPIA kan bepaald worden of het verplicht is om een DPIA uit te voeren en op welke aspecten van de gegevensverwerking mogelijke risico's zijn voorzien.

Deze handreiking is bedoeld voor medewerkers die betrokken zijn bij processen of projecten waarin persoonsgegevens worden verwerkt. Met behulp van deze handreiking kunnen zij de Pre-scan DPIA op een efficiënte en gebruikersvriendelijke manier gebruiken. We raden aan om de originele instrumenten naast deze handreiking te houden. De originele instrumenten bieden de nodige context om de vragen goed te beantwoorden. Schakel daarnaast altijd de juiste expertises in bij het uitvoeren van de Pre-scan DPIA.

In deze handreiking worden definities gebruikt die afkomstig zijn uit de AVG en het Model DPIA Rijksdienst. Deze handreiking is ontwikkeld door Privacy Company in opdracht van het PAR-team (Privacy Adviseur Rijksbrede Kaders & Voorzieningen van CIO Rijk) van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

Inhoud van de Pre-scan DPIA

De Pre-scan DPIA wordt uitgevoerd door het beantwoorden van een vragenlijst in een Excel bestand. Op basis van de antwoorden wordt automatisch een risicoscore berekend die resulteert in een van de volgende uitkomsten: 1) DPIA verplicht, 2) DPIA niet verplicht of 3) DPIA niet verplicht, maar wel aanbevolen (overleg met de CPO).

Het Excel bestand waarin de Pre-scan DPIA is opgenomen, bestaat uit de volgende onderdelen:

- **Titelblad:** documentversie.
- **Info:** een beknopte leeswijzer van de vragenlijst.
- **Vragenlijst:** de vragenlijst met de uitkomst van de risicoanalyse en de eventuele opvolgacties.
- **Informatie verwerkingsregister:** informatie over de verwerking die opgenomen kan worden in het verwerkingsregister. Deze informatie wordt automatisch ingeladen uit de vragenlijst, meer specifiek uit de antwoorden op de vragen.
- **Risico:** de uitkomst van de risicoanalyse (wel of geen verplichte uitvoering van een DPIA) en de berekening ervan.

¹ Data Protection Impact Assessment | Kenniscentrum voor beleid en regelgeving Rijksoverheid [\[link\]](#).

2 Vragenlijst

De [Vragenlijst](#) bestaat uit zeven onderdelen (A t/m G) die elk een soortgelijke opbouw kennen in kolommen: de vraag, het antwoord, de onderbouwing van het antwoord (optioneel) en een toelichting op de vraag. Op basis van de antwoorden wordt automatisch per onderdeel of vragenblok een risico berekend (groen – oranje – rood) dat zichtbaar wordt onder de antwoorden. Voor meer informatie zie [G. Berekening](#).

Indien een DPIA verplicht is, kunnen sommige antwoorden uit de Pre-scan DPIA hergebruikt worden in de DPIA. Bij deze vragen wordt verwezen naar de equivalente paragraaf uit het Model DPIA Rijksdienst. Daarnaast leveren o.a. vragen over het doel, de grondslag en de bewaartermijn van de verwerking input voor het verwerkingsregister. Het advies is daarom om alomvattende antwoorden te geven op open vragen. Na voltooiing van de vragenlijst, is de input voor het verwerkingsregister te vinden op de pagina [Informatie verwerkingsregister](#).

De onderdelen van de vragenlijst worden hieronder verder toegelicht.

A. Inleiding / algemeen

Vragen

1	Beschrijving van de verwerking	4	Cloudgebruik
2	Doel van de verwerking	5	Cloudvorm
3	Grondslag van de verwerking	6	Materieel publiek cloudgebruik

- Het doel van deel A is achtergrondinformatie bieden ten aanzien van de verwerking of het geheel van verwerkingen waar je de Pre-scan DPIA voor invult.
- Afhankelijk van bepaalde antwoorden, zoals bijvoorbeeld het antwoord op de vraag of er sprake is van cloudgebruik, zullen latere vragen wel of niet zichtbaar zijn in de vragenlijst.
- De antwoorden in onderdeel A worden niet meegenomen in de risicobeoordeling van de verwerking, maar kunnen wel gebruikt worden voor de invulling van het verwerkingsregister.

B. Gegevensverwerking

Vragen

7	Typen persoonsgegevens	10	Groepen betrokkenen
8	Bijzondere persoonsgegevens	11	Omvang verwerking
9	Gevoelige persoonsgegevens	12	Gebruikersgroepen

- In Deel B wordt een inschatting gemaakt van de gevoeligheid van de verwerking. Deze gevoeligheid wordt beoordeeld aan de hand van de omvang van de verwerking en de gevoeligheid van de persoonsgegevens en betrokkenen. Worden er bijvoorbeeld biometrische gegevens verzameld door een gezichtsherkenningsoftware of gaat het om de gegevens van een jong kind, dan heeft de verwerking van de persoonsgegevens een grotere impact op de privacy dan bij het uitsturen van een nieuwsbrief naar volwassenen.
- Voor een complete inventarisatie van de persoonsgegevens kan de systemen/verwerkingen-methode gebruikt worden. Eerst beschrijf je de verwerking of geheel van de verwerkingen (stappen in hoofdlijnen, betrokken partijen, welke systemen gebruikt worden). Deze algemene omschrijving is als het goed is al gegeven in onderdeel A. Vervolgens beschrijf je de systemen die gebruikt zullen worden (aantal betrokkenen, typen betrokkenen, typen persoonsgegevens, locatie systeem, beheer etc.) Hierdoor kan je je persoonsgegevenshuishouding als het ware plotten.

C. Internationale doorgiften

Vragen

13	Internationale doorgifte	16	Indien sprake van doorgifte: locatie helpdesk
14	Indien sprake is van een cloudgebruik: hoofdkantoor cloudprovider	17	Indien sprake van doorgifte: telemetrie en/of diagnostische gegevens
15	Indien sprake is van een cloudgebruik: opslag persoonsgegevens	18	Indien sprake van doorgifte: mechanisme(s) voor doorgifte
		19	Indien sprake van doorgifte: doorgifte van bijzondere persoonsgegevens

- In deel C wordt een risicoschatting gemaakt op basis van de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER). Indien persoonsgegevens beschikbaar zijn in landen buiten de EER is het beschermingsregime van de AVG niet direct van toepassing en is de kans groot dat de gegevens daar minder sterk beveiligd worden dan in een land binnen de EER.
- Als data exporteur mag je persoonsgegevens doorgeven naar een land buiten de EER indien er een van de volgende doorgiftemechanismen van toepassing is:
 - Adequaateheidsbesluit (art. 45 AVG)
 - Standaard contractbepalingen (SCC) (art. 46 AVG)
 - Binding Corporate Rules (BCR) (art. 47 AVG)
 - Uitzondering uit artikel 49 AVG
- Is de doorgifte gebaseerd op een adequaatheidsbesluit, dan heeft de Europese Commissie besloten dat het niet-EER land adequate waarborgen biedt om persoonsgegevens te beschermen.² Persoonsgegevens kunnen dan zonder extra maatregelen worden doorgegeven.
- Is er sprake van een ander doorgifte mechanisme dan een adequaatheidsbesluit, dan moet je als data exporteur passende aanvullende maatregelen treffen. Het Europese Hof heeft bepaald dat deze maatregelen moeten worden vastgesteld door middel van een Data Transfer Impact Assessment (DTIA).³ Afhankelijk van de antwoorden in deel C, wordt de DTIA toegevoegd aan de To Do lijst onder deel G.

D. Lijst AP

Checklist

Heimelijk onderzoek	Flexibel cameratoezicht
Zwarte lijsten	Controle werknemers
Fraudebestrijding	Locatiegegevens
Creditscores	Communicatiegegevens
Financiële situatie	Internet of things
Genetische persoonsgegevens	Profilering
Gezondheidsgegevens	Observatie en beïnvloeding van gedrag
Samenwerkingsverbanden	Biometrische gegevens
Cameratoezicht	

² De lijst met niet-EER landen waarvoor een adequaatheidsbesluit is genomen: [\[link\]](#).

³ Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, EDPB, versie 2.0: 18 juni 2021 [\[link\]](#).

- De Autoriteit Persoonsgegevens (AP) heeft een lijst⁴ opgesteld met concrete verwerkingen die waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkene opleveren en waarvoor het uitvoeren van een DPIA verplicht is. In deel D wordt deze lijst getoond als checklist die moet worden afgevinkt.
- Soms overlappen de checks uit de AP lijst met eerdere vragen uit deel B en C, omdat de AP checklist niet uitputtend is en daarom wordt ook een aparte risicoanalyse gedaan in deel B en C.
- De hoog risico verwerkingen worden nader toegelicht in de Pre-scan DPIA, in de kolom Toelichting / Opmerking, en in de officiële lijst van de AP.

E. Lijst EDPB

Checklist

Mensen beoordelen met persoonskenmerken (evaluatie of scoring)	Koppelen van datasets
Geautomatiseerde besluitvorming	Verwerking van persoonsgegevens over kwetsbare groepen of personen
Stelselmatige en grootschalige monitoring	Gebruik van nieuwe technologieën
Bijzondere persoonsgegevens of zeer gevoelige persoonsgegevens	Blokkering van een dienst, recht of contract
Grootschalige gegevensverwerkingen	

- Om organisaties en nationale toezichthouders te helpen bij de toets of een verwerking resulteert in een waarschijnlijk hoog risico voor de rechten en vrijheden van een natuurlijk persoon, heeft de European Data Protection Board (EDPB – Voormalig Working Party 29) een lijst⁵ gepubliceerd met negen criteria die gebruikt kunnen worden bij deze toets.
- Soms overlappen de checks uit de EDPB lijst met eerdere vragen uit deel B, C en F, omdat de EDPB checklist niet uitputtend is en daarom ook een aparte risicoanalyse gedaan wordt in deel B, C en F.
- De negen criteria worden nader toegelicht in de Pre-scan DPIA, in de kolom Toelichting / Opmerking, en in de officiële lijst van de EDPB.
- De EDPB is van mening dat voor een verwerking die aan minimaal twee criteria voldoet, een DPIA moet worden uitgevoerd. Deze ondergrens wordt daarom ook meegenomen in de risicobeoordeling van de Pre-scan DPIA (zie voor meer informatie [G. Berekening](#)).
- Indien er aan één van de negen criteria voldaan wordt levert dat een oranje risicoscore op. Een oranje risicoscore staat voor het dringende advies om de FG te consulteren omdat een DPIA aanbevolen wordt.

⁴ Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens, Nr. 64418, 27 november 2019 [\[link\]](#).

⁵ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, ARTICLE 29 DATA PROTECTION WORKING PARTY, wp248rev.01 [\[link\]](#).

F. Overige

Vragen

Algoritme
Basisregistratie

- In onderdeel F worden de vragen gesteld of er sprake is van algoritmegebruik en / of van een verwerking van een basisregistratie. Een algoritme is een stukje softwarecode dat instructies geeft om een bepaald probleem op te lossen en dat meestal wordt ingezet om beslissingen (deels) te automatiseren.
- Beide situaties leveren een risicoscore op die wordt meegenomen in de berekening van de algemene vragenlijst (zie voor meer informatie [G. Berekening](#)).
- Verder zijn de antwoorden op deze vragen van invloed op de To Do lijst die wordt gegenereerd aan het eind van het document onder de uitkomsten over de DPIA-verplichting. Bij algoritmegebruik moet het algoritme worden toegevoegd aan het Algoritmeregister van de Nederlandse overheid.⁶

G. Berekening

- In deel G wordt de uitkomst, wel of geen DPIA-verplichting, van de Pre-scan DPIA getoond.
- Daarnaast bevat het een aanvullend To Do lijstje met opvolgacties. De To Do lijst bestaat uit standaard opvolgacties en extra acties op basis van de ingevulde vragen.

3 Informatie verwerkingsregister

Een van de standaard opvolgacties is de verwerking opnemen in het verwerkingsregister. Op de pagina [Informatie verwerkingsregister](#) staan een aantal verplichte onderdelen van het verwerkingsregister:

- Beschrijving
- Doel
- Grondslag
- Persoonsgegevens
- Bijzondere persoonsgegevens
- Gevoelige persoonsgegevens
- Betrokkenen
- Omvang
- Bewaartermijn

Deze informatie wordt automatisch ingelezen vanuit de vragenlijst en is hierna te gebruiken bij het invullen van de verwerking in het verwerkingsregister.

⁶ <https://algoritmes.overheid.nl/nl> Let op: bij gebruik van een algoritme is mogelijk het uitvoeren van een impact assessment mensenrechten en algoritmen (IAMA) verplicht.

4 Risico(berekening)

De pagina [Risico](#) bevat de berekening van de uitkomst (het "Eindantwoord") van de Pre-scan DPIA. Het linkerdeel bevat de risicoberekening van de algemene vragenlijst en het rechterdeel bevat een totale berekening van alle vragenlijsten.

Voor de berekening wordt onderscheid gemaakt tussen de volgende vragenlijsten:

- Algemene vragenlijst: deel B, C en F
- AP vragenlijst: deel D
- EDPB vragenlijst: deel E

Berekening algemene vragenlijst

Iedere vraag of vragenblok van de algemene vragenlijst kent een eigen risicoscore en berekening. De risicoscore ziet op het aantal bevestigende antwoorden. De berekening ziet op de hoogte van het risico (groen – oranje -rood). De berekening hangt af van de risicoscore. D.w.z. dat indien de score 2 is bij vraag zeven, het een oranje oordeel krijgt (zie figuur 1).

Over het algemeen geldt, hoe hoger de score, hoe hoger de risicoclassificatie.

Vraag 7 score		
Groen	Oranje	Rood
1	>6	NVT
Berekening ↓		
1		Groen

Figuur 1 – Voorbeeld Berekening vraag 7

Totaalberekening

Onder de totaalberekening worden de risicobeoordelingen van de algemene vragenlijst, AP lijst en EDPB lijst weergegeven. De totstandkoming wordt hieronder toegelicht:

- Algemene vragenlijst: een groene risicobeoordeling staat gelijk aan 0 punten, een oranje risicobeoordeling aan 1 punt en een rode risicobeoordeling aan 2 punten. Voor het oordeel of een DPIA noodzakelijk is, op basis van de algemene vragenlijst, worden de punten van de zeven risicobeoordelingen bij elkaar opgeteld. Zodra deze opsomming gelijk aan of hoger dan 4 is, is het oordeel "DPIA verplicht".
- AP vragenlijst: indien er één of meer bevestigende antwoorden zijn gegeven, is het oordeel "DPIA verplicht".
- EDPB vragenlijst: indien er één bevestigend antwoord is gegeven, is het advies om de CPO te consulteren omdat een DPIA aanbevolen wordt. Indien er twee of meer bevestigende antwoorden zijn gegeven, is het oordeel "DPIA verplicht".

Totaalberekening Vragenlijst			
	Groen	Oranje	Rood
	0	1	2
	Berekening ↓		
Vraag 7	Groen	0	DPIA verplicht
Vraag 8	Rood	2	DPIA is niet verplicht
Vraag 9	Oranje	1	DPIA is niet verplicht
Vraag 10	Groen	0	
Vraag 11	Groen	0	
Sectie C.	Groen	0	
Sectie F.	Oranje	1	
		4	

Uitkomst van:

Algemene vragenlijst

AP vragenlijst

EDPB vragenlijst

Berekening ↓

1

Figuur 2 - Voorbeeld Totaalberekening

Eindantwoord

Om tot een finaal antwoord te komen, wordt er gekeken naar de uitkomsten van de drie vragenlijsten. Is de uitkomst van minimaal één vragenlijst "DPIA verplicht", dan is het finale antwoord van de Pre-scan DPIA ook "DPIA verplicht".

DPIA verplicht	Algemene vragenlijst	
DPIA is niet verplicht	AP vragenlijst	
DPIA is niet verplicht	EDPB vragenlijst	
	Berekening ↓	Eindantwoord
	1	DPIA verplicht

Figuur 3 - Voorbeeld Eindantwoord