Handreiking Pre-scan DPIA

Versie 2.0

Datum 23 augustus 2024
Status Definitief

Inhoudsopgave

1 Inleiding 3

2 Vragenlijst 4

A. Inleiding / algemeen 4

B. Gegevensverwerking 4

C. Internationale doorgiften 5

D. Lijst AP 6

E. Lijst EDPB 6

F. Basisregistraties 7

G. Algoritmes/AI 7

H. Verboden AI systemen 7

I. Hoog risico AI systemen 7

J. Berekening 8

3 Informatie verwerkingsregister 8

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).

Algoritmes, Artificiële Intelligentie (AI) en Kinderrechten

De pre-scan en handreiking zijn het tweede kwartaal van 2024 herzien. Bij deze herziening zijn vragen toegevoegd over het gebruik van algoritmes, AI en de impact op kinderrechten. Hiermee kan de pre-scan ook worden gebruikt om vast te stellen of het wenselijk of zelfs (in de toekomst) verplicht is om een impact assessment uit te voeren voor de toepassing van algoritmes/AI. Daarnaast zijn de pre-scan vragen uit het Kinderrechten Impact Assessment (KIA) ook in deze pre-scan opgenomen.

Het IAMA is ontwikkeld in 2020-2021 en gepubliceerd in de zomer van 2021. In opdracht van het Ministerie van Binnenlandse Zaken heeft een interdisciplinair team van Universiteit Utrecht het IAMA ontwikkeld. In maart 2022 is er een Tweede Kamer motie ingediend en aangenomen die het gebruik van het IAMA verplicht stelt. Het IAMA is beschikbaar in het Nederlands en in het Engels; Fundamental Rights and Algorithms Impact Assessment (FRAIA). Hoewel er andere assessments bestaan die hetzelfde toetsen wordt binnen de Rijksoverheid de voorkeur gegeven aan het IAMA.

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 advies om wel of geen DPIA, IAMA of KIA uit te voeren of daarover verder in overleg te gaan met een Privacy Professional.

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

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 advies of verplichting tot het uitvoeren van diverse assessments) en de berekening ervan.

2 Vragenlijst

De Vragenlijst bestaat uit tien onderdelen (A t/m J) 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 K. 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 gezichtsherkenningssoftware 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 doorgiftemechanismes van toepassing is:
    - Adequaatheidsbesluit (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

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

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	

- De Autoriteit Persoonsgegevens (AP) heeft een lijst[4] 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 lijst[5] gepubliceerd met negen criteria die gebruikt kunnen worden bij deze toets.

---

[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].

[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].

- 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 K. 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 een Privacy Professional te consulteren als overwogen wordt om geen DPIA uit te voeren. Het uitvoeren van een DPIA is in deze gevallen namelijk wel aanbevolen.

F. Basisregistraties

- In onderdeel F wordt gevraagd of er sprake is van een verwerking van een basisregistratie.
- Als er gebruik wordt gemaakt van een basisregistratie levert dat een risicoscore op die wordt meegenomen in de berekening van de algemene vragenlijst (zie voor meer informatie K. 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.

G. Algoritmes/AI

- In onderdeel G worden vragen gesteld die betrekking hebben op de inzet van een algoritme. 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.
- Op dit moment kunnen er per ministerie andere definities van algoritmes gelden. Onder die definities vallen in ieder gevallen systemen die op basis van de AI verordening kwalificeren als een AI systeem. Als het niet duidelijk is wat de definitie is van een algoritme binnen jouw ministerie dan kan je dat navragen bij de Chief Information Officer (CIO).
- Als gebruik gemaakt wordt van een algoritme worden er vragen gesteld over de rol die het algoritme speelt binnen de verwerking. Er wordt ook gevraagd of het algoritme kwalificeert als een AI systeem. Als dat laatste het geval is, moeten de onderdelen H en I ook worden ingevuld.

H. Verboden AI systemen

- Onder de aankomende AI verordening zijn bepaalde toepassingen van AI systemen verboden. De AI verordening zal gelaagd worden geïmplementeerd. De bepalingen die zien op verboden AI systemen zullen als eerste moeten worden nageleefd.

I. Hoog risico AI systemen

- Onder de aankomende AI verordening zijn bepaalde toepassingen van AI systemen gekwalificeerd als 'hoog risico'. Hiervoor gelden aanvullende regels, zoals het uitvoeren van een impact assessment dat ingaat op de impact dat het AI systeem maakt op mensenrechten. Hoewel dit nu nog niet wettelijk verplicht is, is het wel al ten zeerste aan te raden om een dergelijk assessment uit te voeren.
- Als er (vermoedelijk) gebruik gemaakt wordt van een hoog risico AI systeem is het altijd aan te raden om een expert te raadplegen.

- Tot slot zijn er enkele uitzonderingen op basis waarvan een AI systeem toch niet kwalificeert als hoog risico. Ook deze uitzonderingen zijn in de pre-scan opgenomen.

J. Kinderrechten

- In deel J zijn de pre-scan vragen van het Kinderrechtimpact assessment (KIA) opgenomen. Zie het KIA voor meer informatie.

K. Berekening

- In deel K wordt de uitkomst van de Pre-scan DPIA getoond. Er wordt uitgelegd of het wel of niet verplicht is om een DPIA uit te voeren, of het Impact Assessments Mensenrechten en Algoritmes (IAMA) of een andere mensenrechtentoets moet worden uitgevoerd, of het wenselijk is om een Kinderrechten Impact Assessment (KIA) uit te voeren en of het noodzakelijk is om een Data Transfer Impact Assessment (DTIA) uit te voeren.
- 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.

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
- Algoritmes/AI: deel G
- Verboden AI-systemen: deel H
- Hoog-risico AI-systemen: deel I

- Kinderrechten: deel J

Toelichting op het advies:

DPIA-vragen

Of een DPIA verplicht is wordt berekend aan de hand van de onderdelen B, C, F, D en E. Iedere vraag of vragenblok 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 of van de risicoscore.

Afhankelijk van de antwoorden worden in dit deel de volgende adviezen gegeven:

- DPIA is verplicht.
- DPIA mogelijk verplicht, raadpleeg een Privacy Professional.
- DPIA is niet verplicht.

Let op: De uitkomst 'DPIA is verplicht' houdt in dat je wettelijk verplicht bent om een DPIA uit te voeren. Als je twijfelt over de gegeven antwoorden dan kan je dit nader bespreken met een Privacy Professional.

Algoritmes en AI

Voor de onderdelen (G t/m I) wordt ook een risicoscore toegekend op basis van de antwoorden uit de relevante onderdelen. Indien gebruik gemaakt wordt van een verboden AI systeem wordt met klem geadviseerd om geen gebruik te maken van het betreffende AI systeem. Het advies om wel of geen IAMA (of andersoortig assessment dat de inbreuk op mensenrechten toetst) te gebruiken kent een gelaagdheid. Afhankelijk van de antwoorden en uitzonderingen die van toepassing zijn, wordt een van de volgende adviezen gegeven:

- Deze AI-toepassing wordt binnenkort verboden onder de AI-act. Pas dit niet toe!
- Dit is een hoog-risico AI-toepassing. Het wordt onder de AI-act verplicht om een mensenrechtenassessment zoals het IAMA uit te voeren.
- Het algoritme heeft waarschijnlijk een hoog risico. Het advies is om een mensenrechtentoets als het IAMA uit te voeren.
- IAMA of andere mensenrechtentoets voor het gebruik van algoritmen/AI niet noodzakelijk.

Kinderrechten

Bij onderdeel J zijn de vragen van de pre-scan van het Kinderrechten Impact Assessment (KIA) toegevoegd. Afhankelijk van deze vragen wordt geadviseerd om wel of geen KIA uit te voeren. Afhankelijk van de antwoorden wordt een van de volgende adviezen gegeven:

- KIA is aan te raden.
- KIA is niet nodig.
- Zorg voor goede leeftijdsverificatie om te voorkomen dat minderjarigen gebruik maken van de digitale dienst.