



Bezoekadres:

Coolsingel 40, Rotterdam

Postadres: Postbus 70012

3000 KP Rotterdam

Internet: rotterdam.nl/

Van: [REDACTED]

E-mail: [REDACTED]@rotterdam.nl

hoeAan : [REDACTED]

Kopie aan : Privacy office W&I, [REDACTED]

Datum : 15 juni 2021

Betreft : advies DPIA Analytics
uitkeringsonrechtmatigheid

Beste [REDACTED],

Op 10 mei hebben jullie mij advies gevraagd inzake de DPIA Analytics uitkeringsonrechtmatigheid. In deze notitie geeft ik een advies op hoofdlijnen omdat ik van mening ben dat deze DPIA nog niet voldoet aan de AVG.

Ik licht dat hieronder toe.

De DPIA Analytics uitkeringsonrechtmatigheid betreft het gebruik van algoritme voor een selectie van herbeoordeling rechtmatigheid uitkeringen. Het gebruik van algoritme kent veel ethische aspecten en is de laatste jaren stevig onderwerp van discussie. Het gebruik van algoritme heeft extra aandacht vanuit de AP en onlangs is er een zeer kritisch rapport van de Rekenkamer verschenen met expliciete vermelding van dit algoritme. Wij hebben bij onze beoordeling van deze DPIA, de rapportages van diverse recente onderzoeken en aanbevelingen als normkader gebruikt om advies te kunnen geven zodat de toepassing van dit algoritme de algemene toets der kritiek kan doorstaan.

Naast onze inhoudelijke opmerkingen is er nog een extra zorgelijk punt, namelijk dat het gebruik van dit algoritme al in 2017 is gestart en de verwerking die gebruik maakt van dit algoritme niet vermeld is in ons verwerkingsregister. De basis om in control te komen is dat je inzichtelijk hebt welke verwerkingen van persoonsgegevens er plaatsvinden en zeker wanneer er risicogevoelige instrumenten worden gebruikt. Het niet in beeld hebben is een omissie.

Samenvatting:

- De DPIA is **(nog) niet** correct uitgevoerd;
- De DPIA voldoet **(nog) niet** aan de AVG;
- Een voorafgaande raadpleging is momenteel niet opportuun;

Algemeen



De DPIA is een van de belangrijkste onderdelen van de AVG. Doel van de DPIA is de risico's van een verwerking van persoonsgegevens in beeld te brengen, voordat die verwerking plaatsvindt. Een DPIA is wettelijk verplicht bij verwerkingen met een hoog privacy risico. Het gaat daarbij om risico's op gebied van privacy en informatieveiligheid van de verwerking voor betrokkenen (degenen wiens persoonsgegevens worden verwerkt). Een uitgevoerde DPIA moet inzicht geven in deze risico's, maar ook in de maatregelen die de verantwoordelijke moet nemen om deze risico's zoveel mogelijk af te dekken.

De scope van de DPIA

De verwerking ziet op het gebruik van een voorspellend algoritme. Het doel van het voorspellend algoritmemodel is om in te schatten bij welke werkzoekenden het risico dat er te veel of ten onrechte bijstand wordt verstrekt, relatief groot of juist relatief klein is.

Volgens de DPIA is het algoritme al vanaf 2017 in gebruik, maar is tot op heden niet opgenomen in het verwerkingsregister. Evenmin is de verwerking opgenomen in het IBP. De vorige DPIA is gemaakt in 2017 en 2018 en betrof – Pilot Prestatie010. Het algoritme wordt sindsdien gebruikt, maar heeft altijd de status Pilot gehouden, terwijl het volgens de beschrijving van de DPIA als volwaardig instrument in de bedrijfsvoering is toegepast. Het ontbreken van een verwerkingen in het verwerkingsregister zien wij als een belangrijke omissie.

Reden uitvoeren DPIA

Voor deze verwerking is het invullen van de PRA niet toegepast omdat de conclusie is getrokken dat er sprake is van een grootschalige verwerking van gevoelige gegevens van een kwetsbare doelgroep in verband met rechtmatigheidsonderzoek. Hierbij wordt een voorspellend algoritmemodel gemaakt, getraind en toegepast op het uitkeringsbestand.

Is de DPIA correct uitgevoerd?

Uit de DPIA-rapportage blijkt dat personen vanuit verschillende disciplines aan de DPIA hebben meegewerkt. Het gaat om personen met een juridische, informatiserings- en een inhoudelijke achtergrond. Onduidelijk is of de zij akkoord zijn met de DPIA.

Er is gebruik gemaakt van het Rotterdams DPIA model. Het model raakt alle facetten van de AVG.

Kanttekening

In DPIA zijn de maatregelen nog niet opgenomen in hoofdstuk 7. De planningsmatrix is (nog) niet ingevuld

Conclusie:

Met inachtneming van de bovenstaande kanttekening is de DPIA is (nog) niet correct uitgevoerd.

Voldoet de DPIA aan de Algemene Verordening Gegevensbescherming (AVG)?

De AVG geeft aan dat een DPIA minimaal aan de navolgende eisen moet voldoen:



Een systematische beschrijving van de beoogde verwerking (grondslag, juistheid gegevens) en de doeleinden (doelbinding) en een beoordeling van de noodzaak en de evenredigheid (dataminimalisatie). Daarnaast een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen en een overzicht van beoogde maatregelen om deze risico's aan te pakken (bescherming, transparantie).

Beschrijving:

Het doel van de verwerking staat in de DPIA beschreven. Het beoogde resultaat is een beter en sneller inzicht in potentiële onrechtmatigheidsgevallen bij bijstandsverstrekking, waardoor een verhoogde efficiency wordt bereikt:

- Enerzijds door vermindering van gemeentelijk geld dat onterecht wordt uitgekeerd aan bijstand;
- Anderzijds door een effectievere inzet van de beschikbare capaciteit voor handhaving, waardoor er een hogere pakkans is voor fraudeurs en complianten burgers minder worden belast.

Het doel is duidelijk en vanuit het oogpunt van bedrijfsvoering begrijpelijk, anderzijds hebben wij te maken met een zeer kwetsbare doelgroep waar transparantie en eerlijkheid van groot belang is. Het beschermen van de belangen van de betrokkene (Enerzijds een groot maatschappelijk belang voor een efficiënte bedrijfsvoering en juist gebruik voor overheidsmiddelen tegen de nadelen van de burgers die obv een computerprogramma worden uitgezocht en dan voor een ingrijpend heronderzoek in aanmerking komen.) is in de DPIA onvoldoende duidelijk gemaakt.

De beoogde verwerking wordt **niet** afdoende/eenduidig beschreven in de DPIA.

Grondslag:

Er is een aanwezige wettelijke grondslag. In de DPIA wordt hier het volgende over aangegeven:

Artikel 6, lid 1, sub e AVG: taak van algemeen belang:

Participatiewet (o.a. art. 7, 17, 53a lid 6, 64), IOAW/Z (o.a. 13, 14, 44, 45), Wet Suwi (o.a. art. 54, 62), Wetboek Strafvordering (art. 141) en de Algemene wet bestuursrecht. artikel 6 eerste lid onder f en verenigbaar gebruik onder artikel 6 vierde lid.

Uit betreffende artikelen blijkt onvoldoende dat herbeoordeling is toegestaan en evenmin of het gebruik van algoritme is toegestaan. Geadviseerd wordt om dit beter te motiveren.

Naast de vraag over de rechtmatigheid is een belangrijk onderdeel de proportionaliteit en subsidiariteit. Hier vallen met name de ethische vragen onder. De afweging voor proportionaliteit en subsidiariteit en de ethische aspecten worden nauwelijks toegelicht, maar is voor deze groep van groot belang. De belangrijkste ethische aspecten waar een antwoord op wordt verwacht is hierna opgenomen mede de bevinding.

Vanwege het ontbreken van een Rotterdams normenkader hebben we gekeken naar de normen van de Nationale ombudsman, daarnaast hebben de DPIA gelegd naast de bevindingen van de Rotterdamse Rekenkamer.



Normen nationale ombudsman

Wees duidelijk	
Norm	Toetsing
door het gebruik van data en algoritmen en het doel daarvan in kaart te brengen	Staat niet of nauwelijks beschreven welke afweging, proportionaliteit, subsidiariteit voor de inzet van het algoritme
door vooraf te bepalen wie wanneer en hoe wordt betrokken	Worden de mensen die het betreft betrokken?
door actief, begrijpelijk en toegankelijk te informeren over het gebruik van data en algoritmen	Het is nog onvoldoende duidelijk welke data er in het algoritme zitten. Zijn dit alle data uit een uitkeringdossier?
door juridische en ethische kaders te hanteren en de verantwoordelijkheden vast te leggen	Wat is het juridisch en ethisch kader? Is er een deda uitgevoerd en zijn de verantwoordelijkheden goed belegd?
Wees toegankelijk	
door te weten welke burger zich achter de data bevindt en voor hem/haar bereikbaar zijn	Weten we dit?
door de burger zoveel mogelijk te betrekken	Is de burger betrokken en zo nee, waarom niet?
door open te staan voor vragen en klachten over data en algoritmen	Is er een vraagbaak voor burgers voor dit algoritme? Dit staat genoemd in norm 16, maar is niet uitgewerkt.
door als 1 overheid op te treden	
Wees oplossingsgericht	
door vooraf te bepalen waar data en algoritmen wel en niet voor worden ingezet	Is deze afweging gemaakt
door een 'stopknop' in te bouwen	Is die stopknop er? Het was een pilot die is doorgezet, maar is het tussentijds geëvalueerd? Wanneer wordt het project beëindigd of wanneer gaat het door? Wanneer is het project succesvol? Welke criteria moeten er dan zijn?
door altijd de mogelijkheid voor maatwerk en persoonlijk contact te bieden	Zie norm 16, is er een communicatiestrategie?
door continu in gesprek te blijven en te leren van fouten	Dat zit erin, maar is niet goed beschreven

Rekenkamer relevante aanbevelingen

centrale regisseur (aanbeveling 3)	Wie is dat?
deda (aanbeveling 4)	Zie ook het eerder gestelde
ethiek transparantie, verantwoordelijkheid en	staat nu wat bij norm 16, maar totaal niet uitgewerkt
inzicht burger in keuze voor degene die wordt uitgezocht, navolgbaar zijn van ethische keuzes.	de keuze is dus niet navolgbaar, moet goed uitgelegd worden



eerlijkheid, impact op de burger	is deze algoritme eerlijk?
evaluatie algoritme	werkt het algoritme uit 2017 wanneer is deze proef geslaagd

Naast ethische vraagstukken zijn er nog een aantal AVG aspecten waarover geen of onvoldoende duidelijkheid is.

- Het vraagstuk over volledigheid, juistheid en tijdigheid wordt buiten de scope van deze DPIA gelaten. Bij het gebruik van algoritmen is het van belang dat duidelijk is welke informatie er wordt gebruikt en of dit betrouwbaar is. Dit is relevant voor de selectie en de eerlijkheid. Mijns inziens zit er bij de brongegevens een zware controle. Wanneer vastgesteld is dat de brongegevens betrouwbaar zijn dan is het van belang dat gegevens die overgenomen worden betrouwbaar worden overgenomen, naar mijn idee is dit eenvoudig vast te stellen;
- bewaartermijn is nog niet vastgesteld, ook is niet duidelijk of de informatie verwijderd kan worden. Het is van belang om dit met spoed duidelijk te krijgen;
- voor wat betreft training en instructies wordt aangegeven dat er een leidraad is en dat er aandacht aan besteed wordt. Dit is vaag zeker wanneer het om forse risico's gaat over de rechten van betrokkene. Het is belangrijk om concreet aan te geven wat er gedaan wordt en hoe vanuit het management toezicht wordt gehouden op de goede werking;
- Rechten van betrokkenen, hoe kunnen mensen bezwaar maken tegen het verwerken en hoe wordt de transparantie geregeld;
- informatiebeveiliging is een belangrijk aspect. Belangrijk is dat alle aanbevelingen die in de RIA zijn gedaan worden gerealiseerd en voldoen aan de BIO norm;
- er zijn met verschillende partijen verwerkingsovereenkomsten afgesloten. Het is onvoldoende duidelijk hoe beoordeeld wordt dat de afspraken vanuit deze overeenkomsten worden nageleefd;
- Daarnaast zijn er nog andere kleinere punten, die hebben we aangegeven in de concept DPIA

Als laatste wil ik verwijzen naar een aantal relevante richtlijnen op het gebied van beoordeling algoritmen.

Er zijn hiervoor verschillende mogelijkheden. Bijvoorbeeld de richtlijnen toepassen Algoritmen door overheden:

<https://led.pleio.nl/news/view/5438dd4e-5101-4dde-9d1a-ab58cedff81c/richtlijnen-voor-het-toepassen-van-algoritmen-door-overheden>

Vanuit het Kabinet is vorige week een brief aan de Kamer gestuurd met daarin een handreiking voor non discriminatie by design:

https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z10411&did=2021D22770



Wanneer wij naar deze richtlijnen kijken dan zijn de volgende vragen opportuun:

-in de DPIA wordt aandacht besteed aan vooroordelen. Er worden twee soorten bias onderkend namelijk het subjectieve oordeel van de consulent en het feit dat alleen onderzoeken zijn meegenomen, geen situaties waarin geen onderzoeken zijn uitgevoerd.

De vraag is of dit volledig is. Bijvoorbeeld ten aanzien van taal. Alhoewel de nationaliteit is weggelaten wordt wel de taal als gegeven gebruikt. Daarmee is de kans aanwezig dat daarop wordt geselecteerd. Dit kan hetzelfde effect geven als de nationaliteit. Maar ook het gebruik van de postcode, kan leiden tot vooringenomenheid. Dit vraagt meer aandacht dan nu in de DPIA is afgewogen.

Uit de DPIA blijkt dat de data nog getest gaat worden, maar belangrijk is om vooraf al eventuele bias te onderkennen.

Het betreft hier een DPIA, maar eigenlijk gaat het om de beoordeling van een algoritme. Een klassieke DPIA leent zich minder voor de beoordeling van de toepassing van een algoritme. Wel kan de uitkomst van een losstaande beoordeling van een algoritme worden meegenomen in een DPIA. De (volledige) beoordeling van het algoritme mis ik in de DPIA. Althans, er wordt wel aan gerefereerd maar vrij beperkt. Wat mist is een structurele wijze van beoordeling van het gebruikte algoritme.

Conclusie:

Op basis van de hierboven genoemde punten mag duidelijk zijn dat de DPIA (nog) niet voldoet aan de AVG.

Voorafgaande raadpleging Autoriteit Persoonsgegevens.

Indien uit de DPIA naar voren komt dat de verwerking van persoonsgegevens een te hoog risico oplevert en het niet (voldoende) lukt om maatregelen te vinden die dit risico beperken, dan moet de gemeente vooraf (voordat de gegevensverwerking start) overleg voeren met de Autoriteit Persoonsgegevens (AP). Dit wordt de "voorafgaande raadpleging" genoemd.

In de DPIA worden de risico's voor de betrokkene slechts summier besproken, terwijl er sprake is van het verwerken van een groot aantal persoonsgegevens van een groot aantal betrokkenen inclusief gevoelige en bijzondere gegevens. Het is onvoldoende duidelijk wanneer bovenstaande ethische vragen zijn beantwoord welke restrisico's er overblijven. Het is dus van belang om vragen te beantwoorden of toe te lichten en voor risico's beheersmaatregelen vast te stellen. Eerst hierna kan vastgesteld worden welke risico's overblijven na het nemen van de maatregelen.

Oordeel en advies:

De uitgevoerde DPIA voldoet (nog) niet aan de eisen die de AVG. Ik adviseer om met in achtneming van bovenstaande punten de DPIA aan te vullen. Daarna kunnen wij een definitief advies geven. Ik adviseer om bij het opstellen van de DPIA gebruik te maken van onderstaande checklist.



Met vriendelijke groet,



Bijlage: checklist WP29



Checklist DPIA WP 29	Opmerking
Er wordt een systematische beschrijving van de verwerking verstrekt (artikel 35, lid 7, onder a)):	
1 er wordt rekening gehouden met de aard, omvang, context en doelen van de verwerking (overweging 90);	.
2 de persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden bewaard worden geregistreerd;	.
3 er wordt een functionele beschrijving van de verwerking verstrekt	.
4 de activa waarop persoonsgegevens steunen (hardware, software, netwerk en, mensen, papier of papiertransmissiekanalen) worden geïdentificeerd;	.
5 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): 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:	.
6 een of meer gespecificeerde, expliciete en legitieme doeleinden (artikel 5, lid 1, onder b));	
7 rechtmatigheid van de verwerking (artikel 6);	
8 toereikend, ter zake dienend en beperkt tot wat noodzakelijke gegevens zijn (artikel 5, lid 1, onder c));	.
9 beperkte bewaartermijn (artikel 5, lid 1, onder e));	
Maatregelen die bijdragen aan de rechten van de betrokkenen:	
10 informatie verstrekt aan de betrokkene (artikelen 12, 13 en 14);	.
11 recht van inzage en recht op overdraagbaarheid van gegevens (artikelen 15 en 20);	.
12 recht op rectificatie en recht op gegevenswissing (artikelen 16, 17 en 19);	.
13 recht van bezwaar en recht op beperking van de verwerking (artikelen 18, 19 en 21);	.
Overig	
14 relaties met verwerkers (artikel 28);	.
15 waarborgen omtrent internationale doorgifte(n) (hoofdstuk V);	
16 voorafgaande raadpleging (artikel 36).	.
de risico's voor de rechten en vrijheden van betrokkenen worden beheerd (artikel 35, lid 7, onder c)):	



18 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: a er wordt rekening gehouden met de bronnen van de risico's (overweging 90); b 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; c bedreigingen die kunnen leiden tot onrechtmatige toegang, ongewenste wijziging en de verdwijning van gegevens worden geïdentificeerd; d de waarschijnlijkheid en ernst worden ingeschat (overweging 90);	.
19 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:	
20 het advies van de functionaris voor gegevensbescherming wordt ingewonnen (artikel 35, lid 2);	
21 indien nodig wordt de betrokkenen of hun vertegenwoordigers naar hun mening gevraagd (artikel 35, lid 9).	