

Project Analytics Uitkeringsfraude: Privacy Impact Assessment


Documenteigenschappen

Titel Project Analytics Uitkeringsfraude: Privacy Impact Assessment
Auteur [REDACTED]
Versie 1.0
Versie Datum 20-1-2017

Documenthistorie

Datum	Versie	Aangepast door	Opmerkingen
18-1-2017	1.0	[REDACTED]	Versie pilot gemaakt op basis van PIA labfase en gesprek [REDACTED] en [REDACTED] op 18-1

Project Analytics Uitkeringsfraude: Privacy Impact Assessment

Auteur 

Inleiding

In dit document zijn de privacy-aspecten van het te vervolgen project beschreven, en zijn de vragen uit de modelvragenlijst van NOREA voor een Privacy Impact Assessment beantwoord. Het is een vervolg op de PIA die voor de labfase is uitgevoerd en die als apart document beschikbaar is.

Doelbinding

Het uiteindelijke doel van het project (na de uitrolfase) is om data te gebruiken voor het beter opsporen van onrechtmatigheden in de uitkeringsverstrekking. Dit is een wettelijke taak van de gemeente op basis van de Participatiewet (2015). Om dit doel te bereiken wordt vooralsnog alleen data gebruikt die is verzameld op basis van diezelfde Participatiewet, namelijk de operationele data uit het 'inkomen'- en 'werk'-proces van de gemeente zoals vastgelegd in de systemen Socrates en RMW/RAAK. Als in de toekomst sprake is van het koppelen van andere gegevens zal daaraan een privacy-toets voorafgaan.

Proportionaliteit

Fraude en misbruik van gemeenschapsvoorzieningen zijn zware vergrijpen die een stevige handhaving van de uitvoerder rechtvaardigen. Bovendien kan een betrouwbaarder voorspelling leiden tot minder belasting van compliante burgers door minder onterechte onderzoeken. Desalniettemin wordt in het project veel aandacht besteed aan borgen van proportionaliteit. Analytics en machine learning gebruiken in beginsel vaak zoveel mogelijk data juist om onvermoede verbanden te kunnen opsporen. Voor het ontwikkelen van het model gebruiken we zoveel als mogelijk velden juist om te onderzoeken in welke van die velden de voorspellende waarde verborgen zit. Als dat bekend is kunnen we in de loop van de pilotfase richting de uitrol (als we echt de resultaten gaan gebruiken in de praktijk) met veel minder informatie toe; als er een model uitgerold wordt en in beheer wordt genomen worden daarin uiteindelijk alleen die velden gebruikt waarvan gebleken is dat ze een voorspellende waarde hebben. Zo bewaken we proportionaliteit.

Anonimisering en toegestane gegevensvastlegging

Voor de doelstelling van de labfase was het in orde om met zoveel mogelijk geanonimiseerde data te werken, omdat we in die fase nog geen actie koppelen aan de voorspellingen maar alleen een model ontwikkelen. Het was praktisch niet mogelijk om de data volledig te anonimiseren, vooral vanwege de vrije tekstvelden met gespreksverslagen die zijn onderzocht. Daarin zit in sommige gevallen zoveel informatie verborgen dat hij met wat moeite tot identificatie kan leiden. Bovendien bestaat er een geringe kans dat hierin gegevens vastgelegd zijn die niet direct verband houden met de uitvoering van de participatiewet en dus niet verzameld/vastgelegd hadden mogen zijn. Het team let hierop en bij twijfel wordt de privacy-officer ingelicht.

In de pilotfase die van start is gegaan op 1-1-2017, is de doelstelling om aan te tonen dat de in de labfase behaalde resultaten standhouden in de praktijk met echte onderzoeken. Het model wordt daartoe verder doorontwikkeld en er worden daadwerkelijk onderzoeken uitgevoerd waarvan de resultaten worden vastgelegd en vergeleken met de huidige werkwijze(n). Hiertoe moeten deze (enkele honderden) gepseudonimiseerde BSNs weer worden omgezet in echte BSNs ten behoeve van het onderzoeksteam. Dit zal door de verantwoordelijke voor de pseudonimisering gebeuren en de zo ontstane lijst zal geen verdere kenmerken van de personen bevatten om de gevoeligheid van het bestand te minimaliseren.

Informatiebeveiliging

Het model wordt ontwikkeld op de in opdracht van de gemeente ingerichte laboratoriumomgeving in een beveiligde cloud. De beveiligingsmaatregelen voor deze omgeving zijn via een risico-assessment gekozen en goedgekeurd door de security officers van W&I en BCO. Alleen direct bij het project betrokken personen krijgen toegang tot de gegevens en de opdrachtgevers geven daarvoor vooraf

toestemming. Autorisaties worden door de opdrachtgever beheerd. Daarbij geldt het principe dat alleen personen waarbij toegang noodzakelijk is voor het project autorisaties krijgen. Alle medewerkers zijn zich bewust van de gevoeligheid van de gegevens en gaan hiermee zorgvuldig om.

Beantwoording vragenlijst Privacy Impact assessment Labfase Analytics Uitkeringsfraude

Hieronder worden de vragen voor een Privacy Impact Assessment beantwoord. Dit gebeurt specifiek voor de labfase van het project. Voor elke vervolgfase zal deze vragenlijst opnieuw worden ingevuld en beoordeeld.

1 Het type project

1.1 Is er sprake van het verwerken van persoonsgegevens?

Ja. Er wordt zoveel als mogelijk geanonimiseerd (en gepseudonimiseerd) direct bij de bron; BSNs worden niet meegezonden (maar gepseudonimiseerd), geboortedata worden op geboortjaar afgekort, van postcodes worden alleen de cijfers meegegeven etc. Echter, de vrije tekstvelden met gespreksverslagen bevatten grote hoeveelheden gegevens waarin mogelijk ook persoonsgegevens zoals e-mailadressen en mogelijk BSNs verwerkt zijn.

1.2 Is het duidelijk wie verantwoordelijk is voor de verwerking van gegevens?

Ja. Het project wordt uitgevoerd in opdracht van [REDACTED]. Het project wordt begeleid door een begeleidingsgroep met de opdrachtgever, de afdelingsmanager van OBI en externe experts van de Hogeschool Rotterdam en Accenture.

1.3 Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel treedt uw organisatie op als bewerker?

Nee.

1.4 Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?

Ja. Gedurende en na afloop van de pilotfase worden de resultaten en maatregelen geëvalueerd door de begeleidingsgroep. De opdrachtgever zal in overleg met de afdelingsmanager OBI beslissen of het project wordt voortgezet in uitrolfase en welke (aanvullende) maatregelen nodig zijn.

1.5 Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?

Ja. In de pilotfase van dit project wordt het in de labfase reeds ontwikkelde model verder verfijnd en gevalideerd door middel van het uitvoeren van enkele honderden rechtmatigheidsonderzoeken. Het doel is om vast te stellen of het model een betere voorspelling kan doen over welke uitkeringen onrechtmatig zijn dan de huidige werkwijze(n), teneinde de effectiviteit van de handhaving te vergroten.

1.6 Is er sprake van:

a. Gebruik van nieuwe technologie?

Nee

b. Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?

Mogelijk; geautomatiseerde analyse van grote hoeveelheden gegevens kan discussie oproepen.

- c. De invoering van bestaande technologie in een nieuwe context?

Mogelijk. Hoewel door de nationale overheid zeer vergelijkbare analyses al enige tijd worden uitgevoerd, is het relatief nieuw voor een overheid.

- d. (Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?

Nee, eventuele verschuivingen in de werkwijze zullen op zijn vroegst plaatsvinden na afloop van een succesvolle pilot en blijven ook dan beperkt: alleen hoe wordt besloten om tot een rechtmatigheidsonderzoek over te gaan zal veranderen; de onderzoeken worden nog steeds op dezelfde manier uitgevoerd.

- e. Een nieuwe verwerking van persoonsgegevens

Nee, de gegevens werden al verwerkt.

- f. Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen.

Nee, er wordt gebruik gemaakt van gegevens die reeds verzameld zijn.

- g. Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.

Nee

- 1.7 Heeft u op alle bovenstaande (a t/m g) nee geantwoord?

Nee

- 1.8 Is er (naast de Wbp) veel wet-en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?

Ja, de Participatiewet regelt de Bijstand

- 1.9 Zijn er veel maatschappelijke belanghebbenden?

Nee

- 1.10 Zijn er bij veel partijen betrokken de uitvoering van het project?

Nee; de Hogeschool Rotterdam en Accenture werken mee aan het project, maar als medewerkers van de Gemeente.

- 1.11 Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?

Ja, reguliere regeling Gemeente Rotterdam.

2 De Gegevens

- 2.1 Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?

Ja, er worden zo min mogelijk gegevens verzameld voor deze fase. In de pilotfase wordt het model verder doorontwikkeld en ook 'dimensiereductie' uitgevoerd. Dit heeft mede als doel om gegevens die niet relevant blijken te zijn in het uiteindelijke model te kunnen uitsluiten.

- 2.2 Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?

De gegevens worden al maximaal gepseudonimiseerd; de in de ongestructureerde tekstvelden verborgen persoonsgegevens worden op het eerst mogelijke moment uitgefilterd en niet verder gebruikt in de analyse. Voor het uitvoeren van de onderzoeken zal een lijst met gepseudonimiseerde BSNs worden terugvertaald naar echte BSNs door de verantwoordelijke bij W&I; deze lijst bevat alleen de te onderzoeken BSNs zonder hun verdere kenmerken en wordt alleen gebruikt door het onderzoeksteam.

- 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)

Ja, dit is ook het doel van het project.

- 2.4 Is sprake van het verwerken van:

a. Bijzondere persoonsgegevens?
Nee

b. Uniek identificerende gegevens?
Nee

c. Wettelijk voorgeschreven persoonsnummers?
Ja, BSNs op de hierboven beschreven beperkte wijze.

d. Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?

Aantekeningen van gesprekken met gemeentemedewerkers en soms e-mailwisselingen.

- 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?

Nee

- 2.5 Verwerkt u gegevens over kwetsbare groepen of personen?

Nee

- 2.6 Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?

De gehele populatie van bijstandsgerechtigden

3 Betrokken partijen

- 3.1 Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere interne partijen betrokken?

Nee

- 3.2 Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere externe partijen betrokken?

Nee, wanneer het project wordt voortgezet zullen eventuele externe medewerkers wederom als gemeentelijk medewerkers worden ingezet.

- 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?

Nee.

- 3.4 Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?

n.v.t.

- 3.5 Worden de gegevens verkocht aan derde partijen?

Nee

4 Verzamelen van gegevens

- 4.1 Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig?

Nee

- 4.2 Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?

Ja, reguliere proces rond aanvraag en beheer van uitkering.

- 4.3 Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?

Ja, op basis van de participatiewet

- 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)?

Ja, verplichte verzameling o.b.v. de wet.

- 4.4.1 Indien u toestemming aan de betrokkene vraagt (opt-in), kunnen de betrokkenen de

toestemming op een later tijdstip intrekken (opt-out)?

Ja, de kandidaat kan altijd afzien van de uitkering.

4.4.2 Is de impact van het intrekken van de toestemming groot voor de betrokkene?

Ja; verlies van uitkering

4.5 Meldt u de betrokkene dat de gegevens worden verzameld?

Ja, regulier proces uitkeringen

4.5.1 n.v.t.

4.5.2 Bij Ja (op vraag 4.5): meldt u de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?

Ja

4.5.3 Bij Ja: (op vraag 4.5): meldt u de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?

Ja.

4.6 Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?

Nee

5 Gebruik van gegevens

5.1 Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?

Ja, de gegevens worden gebruikt om te onderzoeken of de wettelijke taak beter kan worden uitgeoefend door deze nieuwe toepassing.

5.2 Worden de gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?

Nee, ga verder met vraag 5.3

5.2 N.v.t.

5.2.1 N.v.t.

5.3 Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?

Nee; veel velden zijn niet of niet volledig gevuld, mogelijk niet altijd actueel.

5.4 Worden op basis van de gegevens beslissingen genomen over de betrokkenen?

Nee. Beslissingen over de uitkering worden alleen genomen op basis van rechtmatigheids- of

fraudeonderzoeken.

5.4.1 Bij Ja: leveren de gegevens een volledig en actueel beeld van de betrokkenen op?

N.v.t.

5.5 Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?

Ja; Socrates en RMW/RAAk

5.6 Worden de gegevens breed verspreid binnen de organisatie?

Nee

5.7 Worden de gegevens breed verspreid buiten de organisatie?

Nee

5.7.1 Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van het individu?

n.v.t.

5.8 Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?

Ja.

5.8.1 Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?

Nee

5.9 Kunnen de betrokkenen hun gegevens inzien of daarom vragen?

Ja, conform reguliere proces gemeente.

5.10 Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?

Ja, conform reguliere proces gemeente

5.11 Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?

Ja, conform reguliere proces gemeente

6 Bewaren en vernietigen

6.1 Is een bewaartermijn voor de gegevens vastgesteld?

Ja, regulier proces gemeente

6.2 Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?

Ja, regulier proces gemeente

- 6.2.1 Zo ja (op vraag 6.2), 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?

Ja, regulier proces gemeente

7 Beveiligen

- 7.1 Is sprake van intern geformuleerd beleid over het beveiligen van informatie?

Ja, dit is belegd bij de afdeling Bestuurs- en Concernondersteuning IM MO/W&I in de functie van de adviseur informatiebeveiliging, [REDACTED]