GEGEVENSBESCHERMINGSEFFECTBEOORDELING RIJKSDIENST

Anti-fraude monitoring BT portaal m.b.v. Heidi II systeem

Deze gegevensbeschermingseffectbeoordeling is gebaseerd op "***Model Gegevensbeschermingseffectbeoordeling Rijksdienst***"; versie 0.2 voorportalen CIO-beraad, IOWJZ, ICBR; 24 juli 2017.

Inhoud

Historie

Versie	Datum	Veranderingen	Auteur(s)
0.8	13 oktober 2017	Na 0.98 versie van PIA Heidi een nieuw document begonnen PIA Heidi II waarbij de "soll-versie" het startpunt is van de PIA.	Persoonsgegevens (P-gv.)

Versie	Datum	Veranderingen	Auteur(s)
1.0	18 oktober 2017	Nwe versie naar 1.0 bijgewerkt en aangepast om door te geven ter besluitvorming. Heidi II heeft twee functies en wordt alleen nog toegepast voor Belastingdienst/Toeslagen.	Persoonsgegevens

Het model bestaat uit 17 punten verspreid over vier onderdelen. Onderdeel A behandelt de feiten van de voorgenomen gegevensverwerkingen. De beoordeling van de feiten aan het juridische kader komt aan de orde in onderdeel B. Onderdeel C gaat over risico's voor de rechten en vrijheden van betrokkenen en onderdeel D gaat over de beoogde maatregelen om die risico's aan te pakken. Deze opzet is ontleend aan de privacyregelgeving[1]. Het maken van een GEB is een dynamisch proces. Denkbaar is dat antwoorden in onderdeel A (moeten) worden aangepast nadat een beoordeling (onder B) is verricht en de risico's (onder C) en maatregelen (onder D) in kaart zijn gebracht.

De beantwoording van de 17 punten in dit model kan meer of minder gedetailleerd zijn afhankelijk van de aard en omvang van de voorgenomen regelgeving of verwerkingen door de overheid. Wel is het in alle gevallen noodzakelijk om alle punten van het model na te gaan en de gemaakte afweging per punt op te schrijven.

[1] Artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn.

A. Beschrijving algemene kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1 Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Medio 2013 is functionaliteit beschikbaar gekomen in het Toeslagen Verstrekkingen Systeem (TVS) om de IP-adressen te registreren waarmee toeslagaanvragers het Toeslagen-portal (mijntoeslagen.nl) benaderen. De database-functionaliteit om IP-adressen vast te leggen en te ontsluiten wordt "Heidi" genoemd. Het Heidi-systeem is gebouwd met behulp van de database-programma's Splunk en MariaDB.[2]

Het Heidi-systeem maakt het mogelijk vaste en variabele query's uit te voeren op gegevens die worden vastgelegd bij het bezoek op de portal mijntoeslagen.nl. De vaste query's draaien iedere 15 minuten (quickscan) of op langere intervallen (slowscan). Er zijn ook ad hoc query's mogelijk. Er wordt vastgelegd vanaf welk IP adres de bezoeker afkomstig is, welk BSN het betreft en welke schermen worden bezocht.

Het doel van het verzamelen van deze gegevens is om te kunnen traceren of er sprake is van opvallend gedrag wat een indicatie kan zijn voor een verhoogd risico op misbruik van toeslagen. De waarden van de bij het bezoek ingevulde velden worden niet vastgelegd in het Heidi-systeem. Het loggen en beoordelen maakt het vervolgens bijvoorbeeld mogelijk om te zien:

- dat rekeningnummers massaal worden gewijzigd vanaf één het hetzelfde IP adres;
- dat veel aanvragen worden ingediend vanaf één en hetzelfde IP adres (in korte tijd);
- dat vanaf een IP adres wordt gecontroleerd of toeslagen zijn uitbetaald;
- in voorkomende gevallen kan ook DigiD misbruik worden gesignaleerd.

Nadat het Heidi-systeem voor Belastingdienst/Toeslagen beschikbaar is gekomen, zijn voor andere Belastingdienst-onderdelen aanvullende voorzieningen gebouwd aan het Heidi-systeem (o.a. mijnbelastingdienst.nl en SBR). Het Heidi-systeem is 14 september 2017 uit de lucht gehaald waardoor waardevolle gegevens en analyse-mogelijkheden niet meer beschikbaar zijn. Er is daarna gekeken of het Heidi-systeem voor Belastingdienst/Toeslagen separaat weer operationeel kan worden gemaakt. In een eerste aanzet van een PIA daartoe is aangegeven dat een nieuw aansluiten meer kans maakt wanneer het Heidi systeem wordt afgeslankt naar de oorspronkelijke versie en taken waartoe het in de eerste instantie werd opgesteld. Deze afgeslankte versie wordt Heidi II genoemd. Heidi II bevat voor Belastingdienst/Toeslagen:

1. de functionaliteiten die het mogelijk maken om opvallend gedrag op de portal te traceren (IP scannen voor afwijkend gedrag).
2. de functionaliteiten om de data uit Heidi te laden naar het Datafundament Toeslagen om zo met de gegevens de service en het proces van Belastingdienst/Toeslagen te verbeteren (Gedragsanalyse voor procesverbetering).

2 Persoonsgegevens

Som alle categorieën persoonsgegevens op die worden verwerkt en deel ze in onder de typen: gewoon, bijzonder of strafrechtelijk en wettelijk identificatienummer. Geef per persoonsgegeven aan op wie het betrekking heeft.

2.1 Gewone persoonsgegevens

Veldnaam	Bron	Betrekking op
IP adres		Van gebruiker (aanvrager of gemachtigde)
BSN		Aanvrager van betreffende aanvraag
User agent (info over gebruikte browser, gebruikte besturingssysteem, type apparaat)		Van gebruiker (aanvrager of gemachtigde)

[2] Zie beschrijvingen onder 3.

HTTP methode (wifi of draadverbinding of provider)		Van gebruiker (aanvrager of gemachtigde)
Gemachtigde (als niet door aanvrager zelf wordt bezocht)		Persoon met DigiD machtiging van aanvrager
Overige gegevens die worden vastgelegd maar geen persoonsgegevens zijn: – Gebruikte scherm(en) bij bezoek (URL) – Timestamp (datum en tijd)		
Met verrijking van de gelogde gegevens worden de volgende gegevens aangevuld:		
Vanuit open bronnen worden de IP-adressen verrijkt met: 1. geografische locatie achter IP-adres, 2. Informatie of IP-adres geregistreerd staat als kwaadaardig (versturen van SPAM/Malware/Hack activiteiten) 3. af en toe kunnen we a.d.h.v. geregistreerde gegevens weten welke organisatie achter het IP-adres zit, zoals accountancy bedrijven, KO-centra, openbare netwerken zoals bibliotheken en fastfood locaties. Vanuit BVR[3] [4] worden de gegevens verrijkt met: Geboortedatum, Woonadres, Eerste nationaliteit, Aantal BSN's ingeschreven op adres (berekend gegeven)		

2.2 Bijzondere persoonsgegevens

Veldnaam	Bron	Betrekking op
Zijn er niet		

2.3 Strafrechtelijke gegevens

Veldnaam	Bron	Betrekking op
Zijn er niet (meer na loskoppelen van FSV)		

2.4 Wettelijk identificatienummer

Veldnaam	Bron	Betrekking op
BSN		Aanvrager van betreffende aanvraag waarop wordt ingelogd op het portaal mijntoeslagen.nl

[3] BVR staat voor Beheer Van Relaties: interne Brp kopie van de Belastingdienst.
[4] Per 12 oktober opdracht aan SOC om overlijdensdatum, correspondentieadres en tweede nationaliteit niet meer te verwerken.

3 Gegevensverwerkingen

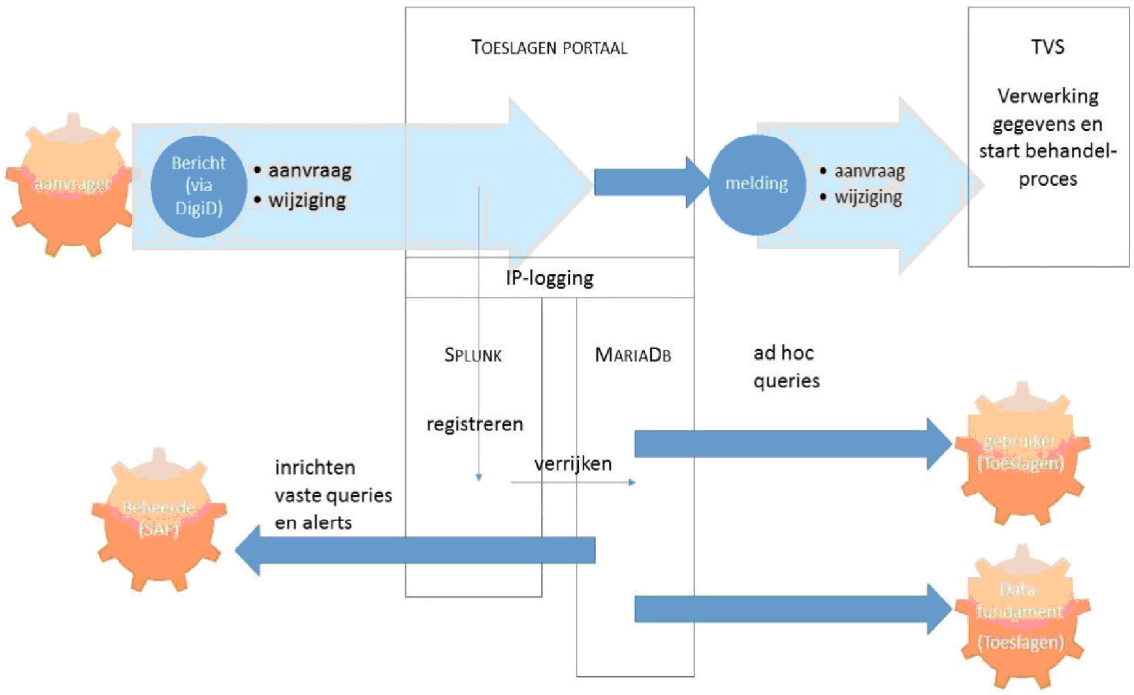
Geef alle voorgenomen gegevensverwerkingen weer.

De activiteiten op het Toeslagenportaal worden gelogd met het databasepakket Splunk. De data, waaronder de persoonsgegevens worden vastgelegd. Splunk logt continu. Iedere dag worden de gegevens vanuit Splunk naar databasepakket MariaDB gekopieerd. In MariaDB worden de log gegevens verrijkt met gegevens vanuit openbare bronnen en de BVR database. Op zowel Splunk als Maria DB draaien verschillende soorten query's. Wanneer deze query's op een situatie stuiten die in een vooraf vastgesteld risicoprofiel past gaat een alert af.[5] Op dat alert wordt een automatische mail verzonden naar enkele contactpersonen met daarin:

1. IP-adres waar activiteit op heeft plaatsgevonden.
2. Gegevens van IP-adres;
3. IP-adres statistieken;
4. De bsn's die onderdeel zijn van de populatie die de treshold overschreed (incl statistische gegevens).

De alerts worden niet opgeslagen in Heidi.

Vanuit MariaDB worden iedere maand gegevens afgegeven aan het Datafundament Toeslagen ten behoeve van analyse op gedrag van toeslagenontvangers. Daar wordt gekeken of bij acties van B/Toeslagen (bijv. versturen brieven dat schattings-inkomen moet worden aangepast) vervolgens een effect valt te zien bij het bezoek aan het portaal.



4 Verwerkingsdoeleinden

Beschrijf de hoofd- en nevendoeleinden van de voorgenomen gegevensverwerkingen.

Zoals ook onder 1 beschreven betreffen de gegevensverwerkingen in Heidi II een tweetal hoofddoelen:

1. IP scannen voor afwijkend gedrag: De verwerkingen ten aanzien van de query's worden gedaan met het doel om opvallend gedrag te signaleren. Dat opvallende gedrag kunnen frauduleuze handelingen zijn of een aanloop zijn naar frauduleuze handelingen. Het gaat dan om systematische fraude ten aanzien van het aanvragen van toeslagen of het opnemen van inkomsten uit toeslagen.
2. Gedragsanalyse voor verbeteren proces: De maandelijkse verwerkingen naar het Datafundament Toeslagen om gedrag van aanvragers te observeren na (massale) acties van B/Toeslagen hebben als doel het monitoren en optimaliseren van de uitvoering van Toeslagen.

[5] Indien het gebruik van een IP-adres een drempelwaarde overschrijdt, wordt er een alert verstuurd per e-mail naar enkele contactpersonen bij Toeslagen/HHR. In deze automatische mail staan gegevens vermeld om het risico op misbruik te beoordelen: is er sprake van opvallend gedrag?

5 Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

1. De vaste query's t.b.v. fraude signalering worden gedaan door de beheerders, een viertal medewerkers van B/CIE SOC[6] (standplaats Apeldoorn). De ad hoc query's ten behoeve van fraude signalering worden gedaan door 4 medewerkers van Data Analyse Toeslagen en 3 medewerkers bij Fraude Team Toeslagen (standplaats Utrecht).
2. De verwerkingen naar Datafundament Toeslagen ten behoeve van gedragsanalyse naar aanleiding van massale acties gebeuren maandelijks handmatig en worden gedaan door de beheerders bij beheerder bij B/CIE SOC, 2 medewerkers bij Data Analyse Toeslagen (v.w.b. ontsluiting) gegevens worden vervolgens beschikbaar gesteld voor 15 data-analisten van Data Analyse Toeslagen, 2 medewerkers van bedrijfsvoering, 3 van productieregie en 3 van IM Toeslagen t.b.v. gedragsanalyses (deze analyses worden ook daadwerkelijk uitgevoerd door ongeveer 6 analisten van D.A.T.).

Het gaat daarbij om verwerkingsverantwoordelijken, om personen die rechtstreeks onder de aansturing van de verwerkingsverantwoordelijke (DGBelastingdienst, dan wel Persoonsgegevens vallen. Iedere gebruiker bevindt zich binnen de Belastingdienst en met name binnen Belastingdienst/Toeslagen. De 4 beheerders B/CIE SOC bevinden zich buiten Belastingdienst/Toeslagen.

6 Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

De verwerkingsverantwoordelijke heeft een wettelijke taak om de inkomensafhankelijke toeslagen juist vast te stellen. Misbruik of fraude moet worden opgespoord en gecorrigeerd. Processen moeten worden geoptimaliseerd.

7 Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Uitsluitend NL (Apeldoorn en Utrecht, zie 5).

8 Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Het Heidi-systeem is gebouwd met behulp van de database-programma's Splunk en MariaDB: Splunk wordt gebuikt om de IP-adressen te registreren en MariaDB wordt gebruikt om de IP-adressen te ontsluiten.
Er is wel sprake van (semi-) geautomatiseerde besluitvorming ten aanzien van de match die optreedt ten aanzien van de gelogde gegevens met de vooraf vastgestelde risicoprofielen.

Er zijn 3 typen vooraf vastgestelde risicoprofielen (alerts) die bij signalering in een query een e-mail sturen (zie beschrijving bij 3) met de geconstateerde gedragingen. Bij de risicoprofielen gaat het om gedragingen vanaf een IP adres die opmerkelijk veel specifiek omschreven transacties verrichten of veel BSN's gebruikt worden via dat IP adres of ongebruikelijk veel bankrekeningnummers worden gewijzigd.

Er is geen sprake van (semi-) geautomatiseerde besluitvorming in de zin van Awb[7]-besluiten. Immers, als het betreffende risicoprofiel optreedt is er menselijke tussenkomst voordat er eventueel sprake is van een gewijzigde beschikking ten aanzien van een toeslag.

Er is wel sprake van profilering en big dataverwerkingen.
Er is sprake van profilering[8] omdat op basis van het gelogde gegevens opmerkelijk gedrag van bezoekers kan worden gesignaleerd. Vervolgens wordt er nader onderzocht of er sprake is van een dergelijke handeling. Hiervoor worden erg veel data verzameld.

[6] Security Operations Center
[7] Algemene wet bestuursrecht, besluiten met rechtsgevolg ten aanzien van een recht op een toeslag of de hoogte van een toeslag.
[8] Artikel 4 onder 4 AVG: "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties,

De verbinding tussen het Heidi-systeem en gebruiker is beveiligd door een encrypted verbinding (SSL). Alle data is encrypted opgeslagen en wordt tijdens het synchroniseren van de data naar Heidi, encrypted over het Belastingdienstnetwerk verstuurd (OpenVPN). Beheerders van Heidi kunnen beheer taken uitvoeren alleen d.m.v. een beveiligde verbinding (SSH). Er wordt gewerkt d.m.v. een need-to-know basis en geen nice -to-know.

9 Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

In de Algemene wet inkomensafhankelijke regelingen (Awir) staat vermeld[9] dat Belastingdienst/Toeslagen (B/T) het organisatieonderdeel van de rijksbelastingdienst is dat belast is met het toekennen, uitbetalen en terugvorderen van tegemoetkomingen. Deze tegemoetkomingen zijn volgens de definitie van deze wet[10]: een financiële bijdrage van het Rijk op grond van een inkomensafhankelijke regeling. Verder bevat de Awir diverse artikelen waarbij onjuiste frauduleuze aanvragen worden gestopt en teruggevorderd en de betreffende aanvrager een verzuimboete of vergrijpboete kan worden opgelegd. Tevens is het mogelijk vermoedens van strafrechtelijke feiten over te dragen aan het Openbaar Ministerie.[11]

10 Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Splunk betreft alleen het logging systeem en bewaart geen gegevens die ouder zijn dan 400 dagen. Na die termijn worden de betreffende gegevens gewist.
In MariaDB heeft geen specificaties voor het wissen van gegevens.
Ten aanzien van de gegevens die worden overgedragen naar het Datafundament Toeslagen bestaan ook geen afspraken of automatische oplossingen voor het wissen van (te) oude gegevens.

Er zijn dus alleen geautomatiseerde voorzieningen ten aanzien van de bewaartermijn van Splunk data. Bij de overige gegevensverwerkingen zijn er (nog) geen afspraken of geautomatiseerde voorzieningen voor het verwijderen van oude gegevens.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11 Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

In de Algemene wet inkomensafhankelijke regelingen (Awir) staat vermeld in artikel 11 lid 2 dat Belastingdienst/Toeslagen (B/T) het organisatieonderdeel van de rijksbelastingdienst is dat belast is met het toekennen, uitbetalen en terugvorderen van tegemoetkomingen. Deze tegemoetkomingen zijn volgens de definitie in artikel 2 lid 1 onder h van deze wet: een financiële bijdrage van het Rijk op grond van een inkomensafhankelijke regeling. Ze worden voornamelijk op aanvraag van een betrokkene verstrekt.
Ten aanzien van fraude is het de taak van de uitvoeringsorganisatie om rechtmatige toekenningen te doen en onrechtmatige of onjuiste toekenningen te herzien. Indien er sprake is van een verzuim, een vergrijp, of een strafbaar feit in relatie met het aanvragen of ontvangen van toeslagen wordt dat ook op basis van o.a. de artikelen uit de Awir[12] door Belastingdienst/Toeslagen afgehandeld. Uit de regelgeving volgt dat strafbare feiten worden overgedragen aan het Openbaar Ministerie.
Ten aanzien van de gedragsanalyse die wordt gedaan om de massale processen te optimaliseren kan ook worden vermeld dat deze kunnen worden gerechtvaardigd op grond van de wettelijke taak van B/T uit de Awir. Voor een goede uitvoering is monitoring en op basis daarvan aanpassing en stroomlijning van de processen van een uitvoeringsorganisatie noodzakelijk.

---

economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen."

[9] In artikel 11 lid 2 Awir.

[10] In artikel 2 lid 1 onder h Awir.

[11] In artikel 44a Awir t.a.v. de contactambtenaar.

[12] Ingevoegd op basis van de Wet aanpak fraude toeslagen en fiscaliteit van 1 januari 2014.

12 Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.

Het gebruik van BSN als identificatienummer is niet wettelijk voorgeschreven bij het aanvragen van toeslagen. Het is wel een algemeen gebruik om bij Belastingen en B/Toeslagen dit nummer te gebruiken bij identificatie en communicatie.

13 Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De persoonsgegevens in het Heidi systeem zijn verzameld met het oog op een soepele en rechtmatige toekenning van toeslagen en worden ook verder verwerkt met dit doel. Met het afslanken van de mogelijkheden en het terugbrengen naar het oorspronkelijke systeem blijft de doelbinding intact.

14 Noodzaak en evenredigheid

Beoordeeld of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de nagestreefde doeleinden. Ga hierbij in ieder geval in op:

1. *Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?*
2. *Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?*

Deze bijna real time monitoring van het portaal is noodzakelijk en effectief gebleken om de, in de voorbeelden genoemde, specifieke fraude op te sporen. Op andere wijze is deze informatie in het geheel niet te krijgen. De gevolgen bij het niet onderkennen van deze fraude is groot (grote bedragen, grote maatschappelijke impact). Er is vaak ook haast geboden indien na analyse blijkt dat er sprake is van een frauduleuze handeling. Er is een impact op de bezoekers van het portaal. De analyses zijn echter niet gericht op individuele aanvragers maar op opvallend gedrag. Als dit gedrag wordt geconstateerd en beoordeeld wordt er actie ondernomen. Er vindt (semi-)geautomatiseerde besluitvorming plaats m.b.v. de gegevens of de constateringen die matchen met de risicoprofielen. Er wordt dan een alert verzonden met de geconstateerde gedragingen. Deze alerts worden niet opgeslagen. De betreffende ontvangen moet vervolgens de alert beoordelen en eventueel actie ondernemen. Er is dus impact maar de gegevens zijn niet op een andere wijze te verkrijgen in deze situaties. Ook de factor tijd speelt mee en zorgt er voor dat geen andere methoden geschikt zijn.
Punt van aandacht is dat betrokkenen niet worden gewezen op het feit dat ten behoeve van profiling gegevens worden opgeslagen en geanalyseerd bij het bezoek aan de portaal mijntoeslagen.nl.

15 Rechten van de betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

Het gedrag van bezoekers op het portaal wordt geprofiled. Hoewel het een ingrijpende maatregel ten aan zien van de bezoekers betreft is het toegestaan op basis van de wettelijke taak van Belastingdienst/Toeslagen. Bezoekers zijn daarvan echter niet op de hoogte. Dat zou wel het geval moeten zijn.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16 Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:

a. *welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van betrokkene;*
b. *de oorsprong van deze gevolgen;*

c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en
d. de ernst (impact) van deze gevolgen voor de betrokkene wanneer deze intreden.

Hou bij elk aspect rekening met de aard, omvang, context en doelen van de gegevensverwerking.

a. Mogelijke negatieve gevolgen op de rechten en vrijheden van de betrokkene

De bezoekers van het portaal mijntoeslagen.nl worden er niet op gewezen dat met het doen van een aanvraag of het wijzigen of inzien van gegevens de gedragingen tevens worden vastgelegd. En dat deze gedragingen worden geanalyseerd (profiling). Dat zou moeten worden aangegeven.
De kans op datalekken van de persoonsgegevens is klein maar aanwezig. Zeker als de persoonsgegevens gedurende lange tijd en in grote hoeveelheden worden bewaard zal een datalek grotere gevolgen hebben.

b. Oorsprong van de mogelijke negatieve gevolgen

Bij het bekend worden van de profiling kan er maatschappelijke commotie ontstaan.
Bij datalekken gaat het om persoonsgegevens.

c. Waarschijnlijkheid (kans) dat de gevolgen zullen intreden

Het feit dat profiling plaatsvindt zal vroeg of laat breder bekend worden. Kans daarop is 100%.
Kans op datalek is minimaal. De verwerking vindt plaats binnen een beperkte omgeving en door een zeer beperkte hoeveelheid specifiek geautoriseerde medewerkers. Verplaatsen van de data gebeurt binnen beschermde omgevingen.

d. Ernst (impact) van de gevolgen voor de gevolgen als deze intreden.

Impact van maatschappelijke commotie is groot gezien de eerdere inbreuken van de Belastingdienst in andere situaties.
Kans op datalek is klein maar de gevolgen daarvan (imagoschade/financiële sanctie) zijn groot.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van betrokkene aan te pakken.

17 Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Het afgeschermde netwerk waar het Heidi II-systeem zich in bevindt, is opgezet d.m.v. privacy by design. Er zit authenticatie, autorisatie en accounting op. Er wordt gelogd en daadwerkelijk actief gemonitord wat gebruikers doen in het Heidi-systeem. Het gaat om een zeer beperkte groep van gebruikers die de benodigde autorisaties bezitten. Betreft daardoor afgesloten data bestanden die niet voor anderen te benaderen zijn.

Eerdere aangekoppelde functies en aanvullingen (FSV) van het Heidi-systeem zijn uit het Heidi II-systeem verdwenen.

Wat er nog zou moeten gebeuren:
Er moet een kennisgeving bij het bezoek van het portaal worden gegeven waar wordt aangegeven dat sprake kan zijn van profiling. Er wordt nog een discussie gevoerd wat voor een soort (statische tekst of wegclicktekst) disclaimer dit moet zijn. Is een kennisgeving noodzakelijk of moet het met clickballon gebeuren. Dat laatste vereist een zwaardere technische aanpassing. Tekst moet ook afgestemd worden. Elders zijn immers nog niet dergelijke disclaimers aangetroffen (!).

Er moet goed gekeken worden hoelang en hoeveel bestanden bewaard moeten worden voor regulier gebruik. De huidige bewaartermijn is lang en de bewaarde bestanden zijn erg groot. Voor het vervolg moeten er dus afspraken gemaakt worden wat, hoe lang en wie/hoe verwijderen?

Er is een voorstel gedaan om de gegevens na 2 jaar in een archief-functie te bewaren en dan 5 jaar in het archief te laten en daarna te verwijderen. Dit sluit aan bij verjaringstermijnen. Van al deze gegevens is het

nodig om in geconstateerde fraude zaken deze informatie nog opvraagbaar en aanwezig voor verdere analyse te laten, zo is aangegeven. Dat kan niet voor het hele gegevensbestand gelden en na afloop van de bewaartermijn kan ook blijken dat een groot deel van de gegevens niet meer gebruikt is. Welllicht kan nader onderzoek uitwijzen of een beperkter bestand van gegevens gedurende langere termijn bewaard moet worden en de rest gewist kan worden.

Memo

	Aanbiedingsmemo behorende bij Gegevensbeschermingseffectbeoordeling (G.E.B.) voor Anti-fraude monitoring BT portaal m.b.v. Heidi II systeem
Aan	RTO, MT
Van	Persoonsgegevens
Datum	20 oktober 2017
Kenmerk	
Kopieën aan	Persoonsgegevens

GEVRAAGD BESLUIT

- Aan het RTO/MT wordt gevraagd de risico's te wegen en te besluiten over het al dan niet gebruik van de voorziening "Heidi".
- Aan B/Cie moet opdracht worden gegeven overeenkomstig het MT beslist

1. ACHTERGROND

In 2013 is op verzoek van het MT-fraude een 'pre-poort[1]' voorziening ontwikkeld door de anti-fraude box samen met B/CIE t.b.v. Toeslagen. Doel van deze voorziening was het afgeven van een signalering op 'afwijkend risicovol gedrag' van bezoekers voor deze TVS portal bereiken. Die voorziening moest een signalering geven vòòr de TVS-portal voor bezoekers met een 'afwijkend risicovol gedrag'. De reguliere pre-poort (Logius) kon die voorziening niet bieden. De voorziening signaleert indicatoren[2] die TVS niet vastlegt. Er is toen, ondanks het van kracht zijn van de WBP, geen PIA. uitgevoerd.

In september 2017 is op gezag van de Persoonsgegevens van DgBel de voorziening on hold gezet omdat deze niet zou voldoen aan de eisen van de WBP. Inmiddels is door vaktechniek Toeslagen een G.E.B. uitgevoerd waarin risico mitigerende maatregelen zijn meegenomen. Er blijven echter rest-risico's.

Het MT wordt dan ook gevraagd de rest risico's te wegen tegen de risico's die ontstaan als de voorziening niet meer kan worden gebruikt. Als bijlage daarom de PIA/GEB die in meer detail de overwegingen schetst.

2. GLOBALE WERKING

Medio 2013 is de functionaliteit Heidi beschikbaar gekomen voor het Toeslagen Verstrekkingen Systeem (TVS). De functionaliteit registreert de IP-adressen waarmee toeslagaanvragers het Toeslagen-portal (mijntoeslagen.nl) benaderen. De database-functionaliteit om IP-adressen vast te leggen en te ontsluiten wordt "Heidi" genoemd.

[1] In 2018 wordt door IV een generieke Pre-poort opgeleverd. Voortgang daarvan moet via IV-Toeslagen worden nagevraagd.
[2] Zie H. 2.1 in het bijbehorende G.E.B.

"Heidi" kent 2 basis functionaliteiten

1. De functionaliteiten die het mogelijk maakt om opvallend gedrag op de portal te traceren (IP scannen voor afwijkend gedrag).
2. De functionaliteiten om de data uit Heidi te laden naar het Datafundament Toeslagen om zo de service en het proces van Belastingdienst/Toeslagen te verbeteren en effecten van handhavingsacties te meten.

Ad. 1
Het doel van het verzamelen van deze gegevens is om te kunnen traceren of er sprake is van opvallend gedrag hetgeen een indicatie kan zijn voor een verhoogd risico op misbruik van toeslagen. Het loggen en beoordelen maakt het onder meer mogelijk om:

- preventief slachtoffers van identiteitsdiefstal te herkennen en hen te behouden voor valse aanvragen op hun naam;
- preventief te signaleren dat rekeningnummers massaal worden gewijzigd vanaf één IP adres hetgeen een indicatie kan zijn van DigiD-misbruik met als doel toeslagen te laten uitbetalen aan een "facilitator";
- preventief te signaleren dat veel aanvragen worden ingediend vanaf één en hetzelfde IP adres (in korte tijd) hetgeen een indicatie kan zijn van DigiD-misbruik met als doel toeslag-gegevens te manipuleren waardoor onrechtmatige toeslagen ontstaan;
- bij het signaleren van (opzettelijk) onjuiste aanvragen (bv n.a.v. valse stukken) of er sprake is van een grotere samenhangende groep aanvragers die nader moet worden onderzocht[3].

Ad. 2
Middels de gegevens uit "Heidi" kunnen de effecten worden gemeten van o.a. de inkomensacties, natuurlijke dialoog, diverse attenderende aan burgers om wijzigingen aan te brengen, monitoren gedragsverandering etc.

3. WAT GAAT ER MIS ZONDER 'HEIDI"?

Er zijn 2 soorten effecten als "Heidi" niet kan worden ingezet.

Ten eerste kunnen zonder de functionaliteiten van Heidi risicovolle gedragingen op de portal niet worden herkent en kan niet preventief worden getoetst. Mogelijke slachtoffers van identiteitsdiefstal kunnen niet worden herkent, onderzoek naar misbruik door samenspanning kan niet meer worden uitgevoerd. Gevolg hiervan is dat onregelmatigheden vaker later in het proces worden ontdekt. Dit leidt tot meer onzekerheid voor burgers, hogere teruggaven, meer rework etc.

Ten tweede kunnen de meeste effectmetingen niet meer plaatvinden. De effectiviteit van preventieve handhavingsacties kan niet meer worden getoetst. Hierdoor zal de Handhaving zich weer vaker manifesteren als toezicht achteraf. Dat toezicht is duur en ineffectief, leidt tot grotere terugvorderingen en meer onzekerheid bij de burger.

[3] Voorbeeld hiervan is onder andere een aantal fraudeonderzoeken waarbij niet alleen bij de voorbereiding door het Fraudeteam maar ook bij de opsporing door de FIOD samenhang kan worden vastgesteld incluis het middelpunt van deze handelingen

4. RISICO'S

Om te kunnen bepalen of het MT Toeslagen de database-functionaliteit Heidi opnieuw wil laten activeren is het van belang om te bepalen of en in hoeverre inbreuk op de privacy en de risico's die daar voor de gebruiker van het Toeslagen portal aan kleven voldoende worden geadresseerd. Uit de PIA/GEB blijkt dat er drietal risico's aanwezig blijven:

- Functioncreep[4]
- Onvoldoende inzicht over de verwijdering en vernietiging van de persoonsgegevens
- Het is vooralsnog onduidelijk hoe en op welke termijn de mededeling, informatie aan de burger dat deze gegevens worden gebruikt, gecommuniceerd zal worden.

Voorgestelde risico mitigerende maatregelen

Functioncreep
Het inrichten van een auditprocedure waarin na 18-24 maanden nadrukkelijk wordt gekeken of de gevraagde persoonsgegevens nog steeds alleen voor Toeslagen en het hierboven beschreven doel worden verzamelt en verwerkt.

Onvoldoende inzicht in de verwijdering en vernietiging van de persoonsgegevens;
Het organisatie onderdeel waar naar verwezen kan worden over die bewaartermijn (B/CIE) vastleggen, dan kan dat als verwijzing in de bij de PIA/GEB behorende onderliggende documentatie worden opgenomen.

De onduidelijkheid over het gebruik van de gegevens richting de burger
Zo snel mogelijk, al dan niet in overleg met P-gv. een duidelijke, eenduidige tekst opstellen en op de diverse sites opnemen.

Het PIA/GEB proces is bedoeld om met elkaar tot een afgewogen risico oordeel te kunnen komen en bij te dragen aan de bewustwording over de voorwaarden waaronder verwerkingen met persoonsgegevens kunnen plaatsvinden. Dat proces heeft plaatsgevonden. Het is nu aan de bestuurder om over de uitkomst te besluiten.

5. GEVRAAGD BESLUIT

Aan het RTO/MT wordt gevraagd de risico's te wegen en te besluiten over het al dan niet gebruik van de voorziening "Heidi". Aan B/Cie moet opdracht worden gegeven overeenkomstig het MT besluit.

[4] Functioncreep is het gebruik van een technologie, een systeem of data voor doelen waarvoor het oorspronkelijk niet bedoeld was. Het helemaal beteugelen van de 'function creep' zal niet gaan; vanuit technologisch perspectief is het een zeer interessant fenomeen en kan het bijvoorbeeld een inspiratie voor innovatie vormen. Het is daarom van belang dat er voldoende andere risicobeperkende maatregelen zijn, worden getroffen.