GEGEVENSBESCHERMINGSEFFECTBEOORDELING (GEB /PIA) RIJKSDIENST

FSV (Fraude Signalering Voorziening)
Geactualiseerde versie 1.2 nov 2019.

Revisiegegevens

Versie	Datum	Auteur	Omschrijving
1.0-1.1	21-01-2019	[redacted]	Initiële versie
1.2	5-11-2019	[redacted]	Geactualiseerde versie

Inhoud

Revisiegegevens..... 2
I. Samenvatting..... 4
II. Vragenlijst Gegevensbeschermingseffectbeoordeling..... 5
A. Beschrijving algemene kenmerken gegevensverwerkingen..... 5
1. Voorstel..... 5
2. Persoonsgegevens..... 5
3. Gegevensverwerkingen..... 6
4. Verwerkingsdoeleinden..... 7
5. Betrokken partijen..... 8
6. Belangen bij de gegevensverwerking..... 8
7. Verwerkingslocaties..... 8
8. Technieken en methoden van de gegevensverwerkingen incl. informatiebeveiliging..... 8
9. Juridisch en beleidsmatig kader..... 10
10. Bewaartermijnen..... 11
B. Beoordeling rechtmatigheid gegevensverwerkingen..... 11
11. Rechtsgrond..... 11
12. Bijzondere persoonsgegevens..... 11
13. Doelbinding..... 13
14. Noodzaak en evenredigheid..... 15
15. Rechten van de betrokkenen..... 16
C. Beschrijving en beoordeling risico's voor de betrokkenen..... 17
16. Risico's..... 17
D. Beschrijving voorgenomen maatregelen..... 18
17. Maatregelen..... 18

I. SAMENVATTING

De (Rijks)Belastingdienst ontvangt en genereert signalen op het vlak van (vermoedens van) fraude[1]. Dit dwingt de organisatie tot een zorgvuldige vastlegging en verdere verwerking van deze signalen. FSV is een voorziening die hierin (mede, naast andere voorzieningen) voorziet.

Uit toetsing middels deze PIA is gebleken dat in zijn algemeenheid kan worden geconcludeerd dat de huidige opzet van FSV geen goede aansluiting (meer) heeft op de verwerkingsbeginselen van art. 5 AVG. Ten aanzien van elk van de in dit artikel genoemde beginselen zijn een of meer bevindingen gedaan en afgeleid daarvan zijn er risico's en maatregelen beschreven.

Als hoofdmaatregel wordt herontwerp/migratie geadviseerd, uitgaande van de blijvende noodzaak om functioneel en processueel te voorzien in geautomatiseerde ondersteuning.

Voor de korte termijn (Q3-4 2019) is een aantal maatregelen beschreven die risicoverlagend zijn. Dit is deels doorgevoerd (beperken aantal autorisaties op basis van toetsing noodzaak tot toegang) of in behandeling (schonen jaarlagen > 7 jaar en beperken massale exportmogelijkheden).

Paragraaf 17 (maatregelen) is geactualiseerd op basis van de stand van zaken per 1 november. De overige onderdelen bevatten, op een enkele redactionale verbeteringen na, de oorspronkelijke beschrijving van januari 2019.

[1] Hier geldt een ruime definitie, alles wat in de 'volksmond' als fraude wordt aangemerkt, dus zeker niet beperkt tot een strafrechtelijke definitie.

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.

Aanleiding voor deze PIA is een opdracht van de directie MKB (MT MKB besluit van 20 augustus 2018) om op basis van de uitkomst van een uitgevoerde WMK-toets (april 2018) een PIA op de applicatie dagboek FSV en het bijbehorende proces uit te voeren. MKB is business en product owner van FSV.

De applicatie Dagboek FSV (Fraude Signalering Voorziening, hierna FSV genoemd) is sinds begin 2014 bestemd voor de registratie van (fraude-)signalen, tips & kliks van derden, informatieverzoeken en hierop gebaseerde projecten[2]. FSV is bij ingebruikname gevuld met de data uit de per 2014 uitgefaseerde applicatie dagboek Persoonsgericht Intensief Toezicht (PIT). Historische gegevens in PIT (dossiers <2010) en de gegevens die tussen 2010 en 2014 in behandeling waren zijn 1 op 1 overgenomen in FSV.

Het betreft registratie van signalen van (vermoedens van) systeemfraude voor meerdere belastingmiddelen en verschillende Toeslagen. Daarnaast wordt de applicatie ook gebruikt voor de registratie van tips & kliks, projecten (per segment, regionaal, plaatselijk) in het subjectgerichte toezicht. FSV wordt ook ingezet voor de registratie van (bijzondere, wettelijke) verzoeken of vorderingen om informatie[3]. Door het vastleggen van deze gegevens, kunnen over een bepaalde periode wellicht bepaalde trends in beeld worden gebracht, bestuurlijke informatie worden verstrekt, en mogelijke andere relevante informatie worden verzameld.

FSV wordt ook gebruikt als bron (middels dumps van de database) voor het voeden van risicomodellen en datafundamenten van DF&A voor bv. IVT en OB-carrouselfraude. Ook voor Toeslagen geldt dat een vermelding in FSV bij inschatting van het risico voedend werkt. Tevens is het een onderdeel van de periodiek toegepaste risicocategorisering. Het procesverloop en in het bijzonder de applicatie dagboek FSV, vormen de scope van deze PIA op een bestaande gegevensverwerking vanuit een eerdere risicoschatting in de voornoemde PIA Informatieloketten. FSV kent vier hoofd-verwerkingsvormen (tabbladen) die waar nodig onderscheiden beoordeeld zullen worden in deze PIA. Dit betreft:

1. Aanmaken/bewerken aangiftefraude[4].
2. Aanmaken/behandelen informatieverzoek.
3. Aanmaken/behandelen Tip/Klikmelding.
4. Aanmaken/behandelen project.

.

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.

In FSV worden van de volgende categorieën betrokkenen persoonsgegevens verwerkt:

1. Belastingplichtigen (al dan niet beschreven) / toeslaggerechtigden;
2. Partner / kinderen van categorie 1;
3. Fiscaal dienstverleners (NP; natuurlijke personen);

[2] Registratie van signalen en informatieverzoeken in FSV binnen MKB is verplicht, op basis van een besluit van het MT-MKB d.d. 24-5-2017.
[3] Er is een directe relatie met de facultatieve PIA Informatieloketten van mei 2018.
[4] Hoewel de titel anders doet vermoeden, betreft het een signaal dat een (*vermoeden van)* mogelijke fraude waaronder aangiftefraude vastlegt. Ook Toeslagen gebruikt deze functionaliteit maar dan voor vermoedens van mogelijke fraude met Toeslagen.

4. Inhoudingsplichtigen (NP);
5. Gastouders (NP); in geval van LRK nummer gastouder.
6. Tip/Klik-meldende personen (al dan niet anoniem);
7. Medewerkers van de Belastingdienst;
8. Medewerkers van andere overheidsdiensten.

	Categorie (detailuitwerking in bijlage 1)	Type
1	NAW gegevens over de persoon	Gewoon
	Gegevens over hardware(locatie) (IP, MAC-adres)	Gewoon
	BSN/RSIN	Wettelijk identificerend
	Sanctie-gerelateerde informatie (bv fiscale boetes)	Strafrechtelijk
	Financiële / fiscale gegevens feiten en objectieve kwalificaties (Negatieve Norm OB; rekenregeluitkomst)	Gewoon / gevoelig
	Strafrechtelijke informatie (van FIOD, OM, Politie)	Strafrechtelijk
	Risico-indicerende kwalificaties mbt voornoemde persoonsgegevens ('besmet adres')	'Zwarte lijst'
	Vrije tekstvelden + bijlagen (ongestructureerde data)	(mogelijk) Gewoon, strafrechtelijke, bijzonder
2	Naamgegevens Partner	Gewoon
	BSN	Wettelijk identificerend
3	Naamgegevens Fiscaal dienstverlener	Gewoon
	BSN	Wettelijk identificerend
4	Naamgegevens Inhoudingsplichtige (NP)	Gewoon
	LH-nr (omvat mogelijk BSN)	Gewoon / Wettelijk identificerend
5	Gastouder(s) ; LRK nummer (Gastouders KOT)	Wettelijk identificerend
6	Naam/info over de Melder/bron Tip/Klik (niet anoniem NP)	Gewoon
7	Naam medewerkers van de Belastingdienst	Gewoon
8	Naam medewerkers van de andere overheidsorganisaties	Gewoon

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Het proces en de voorziening FSV in eerste instantie gericht op de **registratie** van signalen. Primair doel is de **vastlegging** van signalen (tips en kliks, MMA, e.d.), (externe) informatieverzoeken. Hiervan afgeleid ontstaan er mogelijk projecten die met behulp van FSV kunnen worden vastgelegd. FSV wordt belastingdienstbreed gebruikt. Wel wordt er per bedrijfsonderdeel een verschillend gebruik gemaakt (zie 5. Betrokken partijen) en zijn er binnen bedrijfsonderdelen verschillen in het gebruik. Bijvoorbeeld enkele MKB-EOS-teams die alleen algemene signaalinformatie in FSV opvoeren en de (extra vertrouwelijk geachte) details elders **registreren (bijv.** OPO-tool, besloten CP-communities**)**.

Naast registratie van door de Belastingdienst **ontvangen** informatie (denk aan tip/klik signalen) of door medewerkers aangebrachte signalen, wordt FSV ook gebruikt voor signalen die als afgeleide ontstaan van een andere vorm van (persoons)gegevensverwerking bv. de opvraag van fiscale (persoons)gegevens door een andere overheidsinstantie (bv. het OM) die aanleiding geeft om hierover ook een signaal in FSV te **registeren**. FSV heeft een 'signaalfunctie" die bij het opvoeren van een nieuwe signaal aangeeft of er al items in FSV voorkomen. Bij opname van het BSN of RSIN, volgt de melding: "BSN komt x maal voor in FSV". Afhankelijk van het aantal, is het aan degene die een nieuw item opvoert, wat hij/zij doet met de reeds eerder opgenomen informatie[5].

Na registratie vormen **raadplegen, muteren, sorteren, kopiëren** ten behoeve van het primaire proces (individuele klantbehandeling, klantbehandeling toeslagen) en **rapportage-doeleinden** (BI) mogelijke maar, in geval van rapportage/BI, niet veel voorkomende verwerkingen. **Verwijderen, archiveren en vernietigen** is op dit moment alleen gevals-/casusgewijs mogelijk via reguliere systeemfunctionaliteit.

Er zijn tijdens het assessment voorbeelden genoemd van *niet voorgenomen/bedoelde* verwerkingsvormen die functioneel wel mogelijk zijn en worden gebruikt: het **raadplegen** van de werkvoorraad van collega's en het maken van een '**systeemdump**' via de excel-exportfunctie.

Het gebruik van FSV binnen de verschillende bedrijfsonderdelen is niet uniform. Er is een handleiding beschikbaar die een uniforme werkwijze mogelijk maakt.

4. Verwerkingsdoeleinden

Beschrijf de hoofd- en nevendoeleinden van de voorgenomen gegevensverwerkingen.

Voor het uitvoeren van zijn taken op het gebied van uitvoering van heffing en inning, waaronder risicovinding[6], toezicht en handhaving voortvloeiend uit de taken in de Algemene Wet inzake Rijksbelastingen, de Invorderingswet 1990, de Algemene Wet Inkomensafhankelijke regelingen, de Wet aanscherping handhaving en sanctiebeleid SZW-wetgeving 2013 en specifieke (fiscale) middelwetgeving zoals de Wet Inkomstenbelasting 2001, moet de Belastingdienst kunnen beschikken over informatie om de mate van compliantie van belastingplichtigen en toeslaggerechtigden.

FSV draagt bij aan het verrijken van de al beschikbare gegevens, om zodoende te helpen bepalen de mate van compliantie te beoordelen met als doel de mate van (fiscale) aandacht voor een belastingplichtige/ toeslaggerechtigde te bepalen en in voorkomend geval de informatiepositie te verrijken en beter te onderbouwen. De gegevens in FSV hebben het karakter van contra-informatie c.q. renseignementen.

Een tweede doel wordt gevormd door de bestuurlijke informatie en operationele sturingsinformatie die met behulp van FSV kan worden gegenereerd om de inzet van capaciteit, opbrengsten en andere kengetallen inzichtelijk te maken respectievelijk capaciteit zo effectief en efficiënt mogelijk in te zetten. Gebruik (en de mate) hiervan bij de onderscheiden directies, is divers.

Een derde doel vloeit voort uit het voldoen aan wettelijke verplichtingen jegens andere overheidsorganisaties op het gebied van informatieverstrekking[7].

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.

---

[5] Het idee hierachter is, dat 1 klik is geen klik; 2 kliks kan een aanleiding zijn voor (nader) onderzoek, of een richting aangeven aan het behandelen van het nieuwe item.
[6] bv. OB-carrouselfraude, Combiteam Aanpak Facilitators (CAF)
[7] Voor MKB: zie hiervoor de afgeronde PIA op de informatieloketten.

De Minister van Financiën is in beginsel verantwoordelijk voor deze verwerking.

[redacted] zijn als gemandateerd verwerkingsverantwoordelijken aangewezen voor de respectievelijke wettelijke taken.
GO, Douane en FIOD raadplegen FSV voornamelijk. Toeslagen, PDB en MKB raadplegen en muteren in FSV.

De taken in FSV worden feitelijk uitgevoerd door:
- Regiocoördinatoren systeemfraude en IH heffers regionaal
- (fiscale) Baliemedewerkers
- MKB Fraude-EOS-teammedewerkers
- Heffers fiscale middelen en Toeslagen
- Managers heffing en inning en Toeslagen
- Fraudezorgmedewerkers (vorm van slachtofferhulp_ / Stella-teams
- Bezwaren/beroepsprocedure - medewerkers
- Invorderings- en LIC-medewerkers (met name raadplegen)
- AFB (Adviesteam Fraudebestendigheid, voorheen AntiFraudeBox, kan over alle gegevens beschikken);
- DF&A waaronder (voorheen) EHI; (kan over alle gegevens beschikken);
- Douane-medewerkers (2 autorisaties)

De voorziening wordt beheerd door functionele en technische beheerders. In zijn totaliteit zijn ongeveer 5000 gebruikers geregistreerd (waaronder ruim 400 inactieve gebruikers). Dit aantal neemt nog steeds toe.

6. Belangen bij de gegevensverwerking

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

Vanuit het belang van een zorgvuldige en juiste heffing en inning respectievelijk het beoordelen van de rechtmatigheid van de aanvraag en toekenning van toeslagen, worden in FSV signalen vastgelegd. Door het vastleggen van deze gegevens, kunnen over een bepaalde periode (systeem)fraudetrends in beeld worden gebracht, kan bestuurlijke informatie worden verstrekt en relevante informatie op casus- of projectniveau worden verzameld of ter beschikking worden gesteld aan de behandelaar(s). Gedurende het assessment is niet expliciet gebleken dat FSV (consequent) vanuit dit belang wordt gebruikt[8]. De informatieverzoeken worden geregistreerd mede vanuit het belang van zorgvuldig, rechtmatig en doortastend handelende overheid cq andere overheidspartijen veelal met een financiële/materiele invalshoek, bv. binnen een strafproces (OM) of ten aanzien van uitkeringen (UWV) of alimentatieverplichtingen (LBIO).

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.
Nederland; binnen de infrastructuur van het Ministerie van Financiën.

8. Technieken en methoden van de gegevensverwerkingen incl. informatiebeveiliging

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.

Klik hier om infotekst te verbergen

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen

[8] De (voormalige) AntiFraudeBox (AFB) is om deze reden destijds geautoriseerd. Idem EHI.

hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
b. is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
c. berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

a. wettelijk is toegestaan; en
b. voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: 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, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

> De signalen/gegevens worden voornamelijk casusgewijs ingevoerd en opgeslagen in een centrale (SQL)database. Massale invoer van gegevens is mogelijk voor de (platform)beheerder en senior behandelaars voor de 'thema's': aangiftefraude, bijwerken aangiftefraude en project/overig. Het raadplegen en muteren gebeurt primair via systeemfunctionaliteit. Wel is het voor technisch beheerders mogelijk om rechtstreeks de database te benaderen/muteren. Dit wordt niet gelogd en gemonitord.

Er wordt gewerkt met een via IMS-geïmplementeerde autorisatiematrix die de volgende rollen kent:

Baliemedewerker	Senior behandelaar
Medewerker raadplegen	Platform gebruiker / beheerder
Medewerker raadplegen aangiftefraude	Special (BCA)
Medewerker raadplegen B.I.	Behandelaar aangiftefraude
Behandelaar	Senior behandelaar

Er is geen sprake van geautomatiseerde besluitvorming; óf de verwerkte gegevens worden door tussenkomst van een individuele medewerker verwerkt of vormen input voor een verdere verwerking (DF&A, bv. de risicomodellen OB) die niet rechtstreeks leidt tot een geautomatiseerd besluit. De gegevens worden ingezet in big-data-verwerkingsvormen binnen DF&A ten behoeve van de risicomodellen OB (o.m. BTW carrouselfraude). Er is op dit moment binnen de Belastingdienst geen sprake van profilering doordat de Belastingdienst subjectgericht toezicht houdt, in principe gebaseerd op risicoselectie aan de hand van objectieve kenmerken.

Profielen op basis van dergelijke kenmerken worden ingezet voor selectie van dossiers voor toezicht of klantbehandeling. Dergelijke profielen zijn geen product van profilering in de zin van de AVG[9]. Enkele van de binnen FSV verwerkte elementen[10] én het feit dat er ook niet zondermeer objectief getoetste of toetsbare signalen worden geregistreerd, maken dat het karakter van sommige verwerkingsvormen binnen FSV als profilering inclusief 'zwarte lijst'-achtige effecten kunnen gelden. Het überhaupt voorkomen van een betrokkene in FSV wordt bijvoorbeeld gebruikt als signaal in bv. afnemende 'systemen' / verdere verwerkingen (DF&A, mogelijk IVT), zonder dat dit op basis van een objectief aangetoond (verhoogd) risico is gebaseerd (risico van waardering als.. 'waar rook is, is vuur'). Het onderscheid tussen een signaal en een informatievraag wordt bij verdere verwerking ook niet of niet juist gewogen. Niet ieder informatieverzoek is op voorhand een fiscaal signaal.

Er is op dit moment sprake van een lange, op dit moment zelfs ongelimiteerde, bewaartermijn van gegevens. In deze context is ook de kwaliteit van de gegevens van belang (juistheid, volledigheid, actualiteitswaarde). Een niet geverifieerd kliksignaal van een anonieme melder heeft een andere waarde en houdbaarheid dan een objectief aangetoond feit of een als onjuist vastgesteld kliksignaal. De FSV-database bevat signalen die zich begeven tussen beide hiervoor genoemde uitersten. Meerdere rollen (Medewerker BI, behandelaar, senior behandelaar en beheerder) hebben de mogelijkheid, hoewel hiervoor niet bedoeld, om met bestaande systeemfunctionaliteit een export-dump van alle gegevens uit de database te maken. Dit wordt niet gelogd. Vanuit het oogpunt van databeheersing is dit een risico. In totaal zijn 5000+ medewerkers geregistreerd. Daarvan zijn ongeveer 4500 gebruikers actief in FSV, blijkend uit een actuele autorisatie in IMS[11]. Dit aantal herbergt ook een beperkt aantal users dat meerdere malen is opgevoerd. Doordat er niet op basis van een uniek gegeven (zoals UserId) wordt geregistreerd, maar op naam, is vervuiling ontstaan.

Er is geen systeemfunctionaliteit voor het afvoeren van gebruikers. Momenteel zijn er 5-6 functioneel beheerders die medewerkers voor FSV autoriseren op verzoek van IM. De beperkte mate waarin een autorisatieverzoek wordt getoetst op juistheid/toepasselijkheid vormt een risico.
Afgedane posten kunnen gemuteerd worden zonder behoud van het origineel, dus zonder historie en zonder logging. Dit geldt ook voor niet afgedane posten. Medewerkers met mutatierechten kunnen ook posten van anderen muteren. Antidatering van gegevens is mogelijk.

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.

AWR, AWIR, Invorderingswet 1990, middelwetgeving (bv. Wet IB 2001), Fraudewetgeving 2013. Specifieke / sectorale wetgeving van andere ministeries die andere overheidspartijen de wettelijke bevoegdheid geeft bij de Belastingdienst gegevens op te vragen (bv. art. 126 nd Sv, art 23 WLbio, art. 54 WSuwi). De BIR 2017 en het HBB, handboek beveiliging Belastingdienst bevatten het hier toepasselijke beveiligingsbeleid.

10. Bewaartermijnen

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

[9] Standpunt/beslissing DT BD, verslag 7 juni 2018.
[10] Zoals risico-scores of mogelijk subjectieve waarderingen uit andere processen: negatieve-norm OB, prioriteit (2 vormen, nader duiden), besmet adres, besmette postcode.
[11] IMS: identity management systeem; registratie in IMS is noodzakelijk voor toegang in FSV.
[12] En geregistreerd in (Agile)Feature F18.045, Aanpassingen FSV v.0.5, dd. 22-10-2018.

Hoewel procesmatig onderkend[12] bevat FSV geen voorziening om afgedane posten te archiveren gedurende de resterende bewaartermijn om na afloop van de bewaartermijn, gebaseerd op de relevante selectielijst(en), vernietigd te worden.

Op dit moment is alle data toegankelijk en (rolafhankelijk) zowel raadpleegbaar als muteerbaar.

De historie van de geregistreerde data gaat terug tot 2001. Dit wordt mede veroorzaakt doordat bij de start van FSV in 2014 de database van dagboek PIT is geïmporteerd.

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.

1. Verwerking van de persoonsgegevens door de Belastingdienst ten behoeve van zijn wettelijke taken in de fiscaliteit en toeslagen: artikel 6 lid 1 onder e AVG.
2. Artikel 6 lid 1 onder f AVG; gerechtvaardigd belang; hoewel er beperkt voorbeelden[13] zijn gebleken van inzet van FSV trendanalyses en BI ten behoeve van de bedrijfsvoering, is dit wel een beoogde inzetvorm.
3. Registratie van verstrekking op verzoek van persoonsgegevens door de Belastingdienst aan andere overheidspartijen met een wettelijke taak: artikel 6 lid 1 onder c AVG. (de informatieverzoeken). Het volledige proces van de externe informatieverzoeken is behandeld in de PIA Informatieloketten. Hier wordt alleen het aspect registratie (en eventuele verdere verwerking) in FSV bedoeld.

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.

1. **Informatieverzoeken** bevatten mogelijk **bijzondere**[14] persoonsgegevens. De primaire verwerking (het afhandelen van het informatieverzoek) voldoet aan de voorwaarden voor verwerking van art. 9 onder f en g AVG. De verdere verwerking van aangaande het informatieverzoek binnen FSV en evt. andere informatiesystemen moet aanvullend en indien van toepassing herhaald getoetst worden. De context in combinatie met (de betekenis van) de gegevens is bepalend voor de wijze van gebruik. Een informatieverzoek is bv. niet op voorhand / op per definitie een (fraude)signaal en de actualiteitswaarde begrenst. De huidige verwerkingswijze is hierop onvoldoende ingericht.
2. **Tips en kliks**[15] (signalen) ontvangen van derden kunnen **bijzondere** persoonsgegevens bevatten. De Belastingdienst ontvangt en verwerkt deze signalen bij de uitvoering van zijn taken 'spontaan' doordat derden signalen moeten kunnen aanbrengen over andere burgers. De primaire verwerking (het afhandelen van de tip/klik) voldoet aan de voorwaarden voor verwerking van art. 9 onder g AVG. De verdere verwerking is wel aan beperkingen onderhevig incl. dit plicht tot vernietiging bijvoorbeeld bij gebleken onbruikbaarheid of onjuistheid. De huidige verwerkingswijze is hierop onvoldoende ingericht.
3. **Interne en externe**[16] **(fraude) signalen** kunnen **bijzondere** persoonsgegevens bevatten. De

[12] En geregistreerd in (Agile)Feature F18.045, Aanpassingen FSV v.0.5, dd. 22-10-2018.
[13] Toeslagen gebruikt FSV ook om te raadplegen bij Bibob en Track verzoeken. Omdat Toeslagen in FSV het Gefisnr. (th. PSF) registreert en het boetebedrag en percentage in FSV registreert. Dit valt onder het kopje strafrechtelijke gegevens.

[14] Direct of indirect. Bv. in de context van zorgtoeslag kan een gegeven indirect iets over de gezondheidstoestand van een betrokkene zeggen.
[15] Tips/kliks is een algemeen begrip. In het signaal moet worden opgenomen wat de bron. Via overzichten kunnen aantallen (per periode, kantoor, BSN/RSIN) inzichtelijk worden gemaakt.
[16] Zoals MMA, Track/Justis, FIU, iSZW e.d.

primaire verwerking (het afhandelen van de tip/klik) voldoet aan de voorwaarden voor verwerking van art. 9 onder g AVG. In de verdere verwerking speelt de context en kwaliteit van de gegevens een bepalende rol voor de rechtmatigheid en welbepaaldheid van de verdere verwerking. Die is niet voor alle gevallen zondermeer aanwezig. De huidige verwerkingswijze is hierop onvoldoende ingericht. Toeslagen boekt onder "aangifte fraude" de signalen in, op het moment dat er een gerede twijfel is aan de opmaak van documenten (facturen, contracten, etc.) hier is al een kort onderzoek aan vooraf gegaan. Dit kan door een andere afdeling zijn gedaan of afkomstig zijn van externe partijen (zie 4.) of een klikmelding (zie 2.).

4. **Informatieverzoeken** bevatten **strafrechtelijke** persoonsgegevens. De wettelijke uitzondering voor verwerking is primair gelegen in de wettelijke grondslag (lees verplichting) bijvoorbeeld een vordering op grond van art. 126nd Sv. Daarmee voldoet de verwerking 'in enge zin' (ten behoeve van het voldoen aan de vordering) aan de voorwaarden[17] voor verwerking van art. 10 AVG jo art. 23 onder c UAVG. De verdere verwerking binnen FSV en evt. andere informatiesystemen voldoet aan de voorwaarde van 'verwerking onder toezicht van de overheid'. De context van een informatieverzoek in combinatie met (de betekenis van) de gegevens is wel bepalend voor de wijze van gebruik. Een extern informatieverzoek is niet bedoeld te gelden als / niet op voorhand / per definitie een (fraude)signaal en de actualiteitswaarde is begrenst. Toeslagen doet bij gerede twijfel eerst onderzoek en voert dan evt. een signaal op. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd. De aanpak van Toeslagen kan, indien dit past binnen het uitvoeringsproces, hierbij als uitgangpunt worden genomen.
5. **Tips en kliks** ontvangen van derden kunnen **strafrechtelijke** persoonsgegevens bevatten. De Belastingdienst ontvangt en verwerkt dit 'spontaan' doordat derden signalen moeten kunnen aanbrengen over andere burgers. Ook hier is bij aanvang van de verwerking sprake van de uitzondering 'onder toezicht van de overheid'. De verdere verwerking is wel aan beperkingen onderhevig incl. dit plicht tot vernietiging bijvoorbeeld bij gebleken onbruikbaarheid of onjuistheid. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd.
6. **Interne (fraude) signalen** kunnen **strafrechtelijke** persoonsgegevens bevatten (waaronder daarmee gelijkgeschakelde fiscale sanctiegegevens). Ook hier geldt dat bij aanvang van de verwerking strafrechtelijke gegevens sprake is van de uitzondering 'onder toezicht van de overheid'. In de verdere verwerking speelt de context en kwaliteit van de gegevens een bepalende rol voor de rechtmatigheid en welbepaaldheid van de verdere verwerking. Die is niet voor alle gevallen zondermeer aanwezig. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd.
7. Bovenstaande geldt ook voor projecten gebaseerd op gegeven zoals besproken onder 1 tot en met 6.
8. Gegevens met een **'zwarte lijst'**-karakter: in FSV ontstaan of worden bestaande gegevenselementen verwerkt die het karakter van een zwarte-lijst-element hebben of krijgen. De mogelijke subjectiviteit ('bias', vooringenomenheid, zelfversterkend effect door stapeling) maakt het verwerken risicovol. Ook het voorkomen in FSV als betrokkene wordt als risicosignaal. Dit brengt ook een aantal risico's met zich mee waaronder een mogelijk 'zwarte lijst'-effect.

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 vraag of de verdere gegevensverwerking verenigbaar is met het oorspronkelijke verzameldoel van de gegevens, speelt met name met betrekking tot de verdere verwerking gegevens in FSV. De initiële

[17] '..verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unitrechtelijke of lidstaatrechtelijke bepalingen die voldoende waarborgen ... bieden." Zorgtoeslag van Toeslagen is een tegemoetkoming in de kosten voor een zorgverzekering, die inkomensafhankelijk is.

vastlegging van persoonsgegevens bij (registratie van) een informatieverzoek of (extern) tip/klik/signaal of intern signaal is namelijk het begin van de verwerking. Vanwege het verschillende karakter worden informatieverzoeken apart behandeld naast de (fraude)signalen.

Informatieverzoeken: In deze afweging zijn de volgende factoren gewogen:

a. Het verband tussen het oorspronkelijk verzameldoel en de doeleinden van de voorgenomen verdere verwerking;
b. Het kader waarin de persoonsgegevens zijn verzameld en de redelijke verwachtingen van de ontvanger (de betrokkene) met betrekking tot de voorgenomen verwerking;
c. De aard van de persoonsgegevens en met name of bijzondere persoonsgegevens worden verwerkt;
d. De mogelijke gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene);
e. Het bestaan van passende waarborgen, waaronder versleuteling of pseudonimisering van de gegevens.

Ad a. Het informatieverzoek wordt verwerkt (geregistreerd) wanneer een externe overheidspartij op basis van een wettelijke grondslag inlichtingen vordert. Het verwerkingsdoel is tweeledig:

1. Vastlegging van (een deel van de[18]) informatie aangaande het informatieverzoek ten behoeve van een goede verwerking van het verzoek en het creëren van een audit trail.
2. Vastleggen van contra-informatie/renseignementen vanuit het (ten dele statistisch onderbouwde) ervaringsgegeven[19] dat een significant deel van subjecten waarvan informatie wordt opgevraagd, fiscaal gezien aanvullende aandacht verdient of mogelijkheid dat de betrokkene ook fiscaal nader onderzocht of getoetst moet worden. (Vermoedens van) misbruik doet zich veelal regeling overstijgend voor én er is een wederzijdse relatie doordat inkomen- en vermogen (mede)bepalend is voor aanspraken op diverse regelingen buiten de fiscale context.

De verdere verwerking zal plaatsvinden doordat bij de risico(posten)selectie en/of individuele klantbehandeling FSV direct of indirect (via export van FSV-data naar andere bronnen) wordt geraadpleegd. Het gebruiken van FSV als bron is verenigbaar indien kan worden gegarandeerd dat de gegevensset juist, volledig en actueel is en de gegevens inclusief contextinformatie worden verwerkt. Een informatieverzoek heeft bv. een andere context en daardoor betekenis dan een kliksignaal.

[18] In veel gevallen wordt in FSV alleen een signaal vastgelegd en worden onderliggende stukken elders opgeslagen. Dit wordt voornamelijk ingegeven door het grote aantal autorisaties op FSV en het daardoor ontstane overschrijden van een need-to-know-toegang tot signaalinformatie.
[19] Bron: DF&A

Er is vastgesteld dat deze zorgvuldigheid bij de huidige inrichting niet voldoende kan worden gegarandeerd. Zo wordt per bedrijfsonderdeel en daarbinnen per behandelend team (en mogelijk individu) anders omgegaan met de mate van vastlegging in FSV. Ook de verdere verwerking van FSV data in andere informatiesystemen is voldoende fijnmazig. Als het überhaupt voorkomen in FSV als selectiecriterium geldt, wordt geen rekening gehouden met de context en hiervan afgeleid met mogelijk (onterechte) stigmatisering van betrokkenen als gevolg.

Ad b. Het vastleggen van een informatieverzoek vloeit voort uit een wettelijke plicht. De betrokkene zal in het merendeel van de gevallen hiervan niet (direct) op de hoogte zijn maar via het dossier (strafdossier, alimentatie-dossier LBIO) op enig moment geconfronteerd worden met het feit dat een dergelijke verwerking heeft plaatsgevonden. De Belastingdienst informeert de ontvanger (betrokkene) in zijn algemeenheid door middel van het privacy statement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst".

Ad c. Er worden bijzondere- en strafrechtelijke persoonsgegevens verwerkt evenals een wettelijk identificatienummer (BSN). De aard en het karakter van dit type verwerking brengt dat met zich mee. Dit brengt extra zorgvuldigheidseisen met zich mee uitgaande van wettelijke mogelijkheden (zo niet verplichting) om deze gegevens te verwerken.
Ad d. De gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene) kunnen groot zijn. Als de enkele registratie van een informatieverzoek in FSV, zonder fiscale relevantie vervolgens meerjarig (tot nu toe zelfs blijvend vanwege het ontbreken van een verwijdermogelijkheid) geldt als variabele in diverse risicoprofielen van de Belastingdienst, dan herbergt dit het risico van te grofmazige risicoselectie en mogelijke stigmatisering.
Ad e. De gegevens worden verwerkt binnen de beveiligde infrastructuur van de Belastingdienst zonder pseudo- of anonimisering. Het relatief grote aantal personen dat toegang heeft tot de gegevens (raadplegen en evt. muteren, rolafhankelijk) zonder een goed ingerichte need-to-know-structuur en het ontbreken van logging en monitoring vormt daarbinnen een risico.

(Fraude/klik/tip)Signalen: De signalen vormen de tweede groep die beschouwd zal worden in deze paragraaf. Hoewel verschillend qua typologie vormen ze wel één groep die zich onderscheidt van de informatieverzoeken.
Ad a. De geregistreerde signalen van fraude/misbruik worden gebruikt voor (ruwweg) risicoselectie en de klantbehandeling. Bij signalen van derden ligt het initiatief bij (anonieme) burgers en komen van andere (overheids)Partners af, interne signalen komen op vanuit de verschillende bedrijfsprocessen rondom de klantbehandeling (fiscaal en toeslagen). Verwerking vindt steeds plaats in de context van het bevorderen van compliantie van betrokkenen.
Ad b. Hoewel de Belastingdienst de betrokkene in zijn algemeenheid informeert door middel van het privacy statement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst", is de specifieke verwerking van signalen in FSV voor het merendeel van de betrokken onbekend. Indirect wordt een betrokkene hier op enig moment mee bekend doordat er een vorm van (geïntensiveerde) klantbehandeling ontstaat waarin FSV mede bepalend is geweest.
Ad c. Er worden mogelijk en in voorkomend geval bijzondere en strafrechtelijke persoonsgegevens verwerkt evenals het BSN als wettelijk identificatienummer.
Ad d. De gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene) kunnen groot zijn. Als de enkele registratie van een signaal in FSV leidt vervolgens meerjarig (tot nu toe zelfs blijvend vanwege het ontbreken van een verwijdermogelijkheid) geldt als variabele in diverse risicoprofielen van de Belastingdienst, dan herbergt dit het risico van te grofmazige risicoselectie en mogelijke stigmatisering.
Ad e. De gegevens worden verwerkt binnen de beveiligde infrastructuur van de Belastingdienst. Het relatief grote aantal personen dat toegang heeft tot de gegevens (raadplegen en evt. muteren, rolafhankelijk) zonder een goed ingerichte need-to-know-structuur en het ontbreken van logging en monitoring vormt daarbinnen een risico.

14. Noodzaak en evenredigheid

Beoordeeld of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de nagestreefde doeleinden.

a. Proportionaliteit:
Vanwege het verschillende karakter worden ook hier informatieverzoeken onderscheiden behandeld van de (fraude)signalen.

Informatieverzoeken: de inbreuk op de privacy wordt gerechtvaardigd doordat de afhandeling van een informatieverzoek voortvloeit uit een wettelijke plicht. Vanuit een zorgvuldigheidsoogpunt is registratie een noodzakelijke processtap. De noodzakelijkheid van de (verdere) verwerking buiten de 'logistieke' doeleinden van het zorgvuldig afhandelen van een informatieverzoek vraagt om aanvullende, privacy-bevorderende maatregelen. De noodzaak van verdere verwerking van een informatieverzoek als renseignement moet zorgvuldig worden getoetst én vraagt om vastlegging van voldoende (en hierdoor mogelijk verwerking van meer) (persoons)gegevens om bij de verdere verwerking de relevantie te kunnen bepalen. Tevens moet de 'houdbaarheid' voldoende fijnmazig worden bepaald. Ieder (type) informatieverzoek heeft zijn eigen, beperkte, actualiteitswaarde. Er moet een goed evenwicht gevonden worden tussen ervaringsregels als 'een signaal is geen signaal' en 'waar rook is, is vuur' die ieder voor zich leiden tot het verlengen van de bewaartermijnen en de belangen en rechten van betrokkenen. De werkwijze van Toeslagen, waarbij een informatieverzoek wordt 'gewogen' en bij gerede twijfel FSV wordt 'aangevuld' met een signaal lijkt een zuivere scheiding tussen een informatieverzoek en een signaal te kunnen aanbrengen.

(Fraude/klik/tip)Signalen: de inbreuk op de privacy wordt in zijn algemeenheid gerechtvaardigd doordat het ontvangen of intern ontstaan van signalen een logisch gevolg is van de uitvoering van de wettelijke taken van de Belastingdienst. Signalen van derden (tips/kliks en andere signalen) zijn vormvrij, wat maakt dat een uniforme vastlegging georganiseerd moet worden. FSV is hiervoor een instrument. De criteria voor registratie in FSV laten toe dat de mate van 'hardheid', objectiviteit / subjectiviteit, bruikbaarheid en actualiteit per melding verschilt zonder dat dit in de verdere verwerking als objectieve criteria toetsbaar is. Dit vraagt om aanvullende, privacy-bevorderende maatregelen die een betere balans geven in de plicht om een zo beperkt mogelijke privacy-schending te veroorzaken en tegelijkertijd de noodzaak tot het registreren van (mogelijk) fiscaal relevante signalen blijvend mogelijk te maken.

b. Subsidiariteit:
De verwerkingsdoelen voor beide informatiestromen kunnen met een aangepaste verwerkingswijze in FSV leiden tot hetzelfde resultaat maar met een minder grote inbreuk op de persoonlijke levenssfeer van betrokkenen. De mate waarin dit in de huidige opzet van FSV mogelijk en wenselijk is of bv. in de vorm van een migratie naar een nieuwe omgeving/voorziening, zal nader beoordeeld moeten worden.

De belangrijkste aspecten, grotendeels corresponderend met de hierna in paragraaf 16 te benoemen risico's, zijn: het aanbrengen van een beter onderscheid tussen informatieverzoeken en 'echte' signalen. de bewaartermijn, registratie en meeleveren van metadata (contextinformatie) ten behoeve van de verdere verwerking en need-to-know/have toegang van medewerkers.

.

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 karakter van de verwerkingsgrondslagen voor opname van (persoons)gegegevens in FSV zal er in veel gevallen toe leiden dat bij een eventueel inzageverzoek betrokkene geen specifieke informatie, zoals verwerkt in en vanuit FSV, zal ontvangen. Een wettelijke geheimhoudingsplicht (bijvoorbeeld voortvloeiend uit art. 126nd SV maar ook specifieke signalen zoals MeldMisdaadAnoniem) kan hieraan in de weg staan maar ook de voorlopige geheimhouding corresponderend met de wettelijke taken van de (rijks)Belastingdienst. Art. 23 AVG, in het bijzonder letter d en h AVG geldt hier als beperking op de rechten van betrokkene.

Wel informeert de Belastingdienst de ontvanger (betrokkene) in zijn algemeenheid met betrekking tot in FSV registreerde persoonsgegevens door middel van het privacystatement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst".

.

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.

1. In zijn algemeenheid kan worden geconcludeerd dat **de huidige opzet van FSV geen goede aansluiting (meer) heeft op de verwerkingsbeginselen van art. 5 AVG.** Ten aanzien van elk van de 10 in dit artikel genoemde beginselen zijn een of meer bevindingen gedaan en afgeleid daarvan zijn er privacy risico's gesignaleerd. Hieronder worden de meest impact hebbende risico's beschreven. De hoofdmaatregel genoemd in .17 sluit overigens specifiek aan op dit eerste 'meta-risico'. Dit staat los van de behoefte aan (noodzaak tot) een voorziening en proces voor het zorgvuldig en veilig verwerken van (fraude)signalen.

2. **Onvoldoende onderscheid tussen een informatieverzoek en een signaal maar ook betekenis/gewicht van de informatie, leidt tot mogelijke stigmatisering van betrokkenen ('zwarte lijst effect').** FSV biedt de mogelijkheid tot registratie van beide fenomenen wat bij de (verdere) verwerking, afhankelijk van de wijze van verwerking, door de individuele gebruiker (of bedrijfsonderdelen) tot een verschillende en deels risicovolle verwerking leidt. Een afgeleid risico ontstaat doordat er nauwelijks of geen onderscheid wordt gemaakt in de kwalificatie, 'gewicht' en betekenis van een melding. Een informatieverzoek zonder fiscale relevantie 'weegt' even zwaar als een 'vage' klikmelding ('buurman drie keer met een aanhangwagen met 'handel' zien rijden') of een concrete melding van bv. een valse factuur. Zeker wanneer de FSV content integraal (verder) wordt verwerkt en/óf de registratie in FSV als risicofactor wordt (mee)gewogen, is de kans groot dat een deel van de betrokkenen onterecht of bovengemiddeld snel/vaak als risicopost wordt aangemerkt met als gevolg een mogelijk meer intensieve klantbehandelingsvorm dan noodzakelijk is.

[20] Waarvan ongeveer 10% (509) inactief, dd dec 2018.
[21] Fenomeen dat ontstaat als personen zich anders gaan gedragen vanwege een mogelijke privacy-impact. Doorgaans betrokkene (belastingplichtigen), in dit geval medewerkers.

3. **De datakwaliteit vormt een risico** doordat registratie in FSV niet uniform geschiedt, het onderscheid tussen objectieve en subjectieve informatie onvoldoende inzichtelijk is en verouderde informatie blijvend wordt verwerkt. De oorzaak van voornoemde voorbeelden is verschillend. Respectievelijk de verschillende werkwijze van bedrijfsonderdelen (én teams en per medewerker), feiten en vermoedens (waaronder het label 'besmet adres') die deels zonder nadere kwalificatie/onderscheid worden verwerkt en het ontbreken van massale-archiverings-/schoningsfunctionaliteit. Dit heeft tot gevolg dat er een incompleet, onjuist en/of gedateerd beeld van betrokkenen ontstaat in de (verdere) verwerking van gegevens, ook buiten FSV, zoals de risicopostenselectie (bv. bij DF&A) en toetsing in FSV in geval van individuele klantbehandeling. Dit kan aanzienlijke nadelige gevolgen hebben voor betrokkenen.

4. **Informatiebeveiligingsissues waaronder onvoldoende garantie ten aanzien van data-integriteit, vormen een risico** door te ruime toegang tot en onvoldoende controle op het gebruik van de gegevens in FSV. Er zijn inmiddels 5000+ medewerkers geautoriseerd[20] voor minimaal raadpleegtoegang tot alle data. Enkele rollen kunnen een export van de volledige database maken zonder zicht op de verdere verwerking van de geëxporteerde data. Er bestaat de mogelijkheid voor medewerkers met muteerrechten tot wijzigen (aanvullen, wijzigen, ante-dateren etc) van alle data in FSV. Dit wordt niet gelogd en gemonitord. Ook leidt voornoemde in zekere zin tot een zgn 'chilling effect'[21] doordat meerdere teams FSV slechts beperkt vullen ('hit-no hit-achtig') en een parallelle administratie voeren voor de details van het signaal. Hoewel er geen voorbeelden van incidenten/misbruik bekend zijn, voldoet de huidige verwerkingsvorm niet aan de eisen die, mede vanuit privacy by design/default, aan informatiesystemen worden gesteld. Ook hier bestaat een aanzienlijke kans dat de inbreuk op de privacy groter is dan noodzakelijk en de impact aanzienlijk kan zijn als er (veelal een verdere) verwerking ontstaat door de wijze van registratie in FSV.

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 besc hreven 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.

Als hoofdmaatregel wordt een herontwerp / migratie van FSV-functionaliteit naar een nieuwe opzet[22] geadviseerd. Daarmee kunnen, met als uitgangspunt privacy by design en default, de gesignaleerde risico's worden weggenomen. Borg daarbij dat de migratie wordt gedaan in combinatie met risicoborgende, processuele maatregelen als procesuniformering[23], work-flow-management en bijvoorbeeld (verbeterd) zicht op en zeggenschap over de verdere verwerking van FSV-data buiten FSV. Herontwerpaspecten gerelateerd aan privacy-risico's zijn dan:

- gegevenskwaliteit: juistheid en metadatering van de betekenis van gegevens waaronder het 'gewicht' van een signaal, bewaartermijn en het onderscheid tussen een signaal en een informatieverzoek;
- doorontwikkelen waaronder mogelijk uitfaseren van systeemfunctionaliteit en verfijnen van de autorisatiematrix;
- organiseren en reguleren van (al dan niet geautomatiseerde[24]) datadistributie;

[20] Waarvan ongeveer 10% (509) inactief, dd dec 2018.
[21] Fenomeen dat ontstaat als personen zich anders gaan gedragen vanwege een mogelijke privacy-impact. Doorgaans betrokkene (belastingplichtigen), in dit geval medewerkers.
[22] Mede ingegeven door de constatering dat er functionele wensen bestaan, soms overlappend met de in de PIA geadresseerde issues, die niet (goed) in de huidige applicatie-architectuur kunnen worden uitgewerkt. Kostenefficiëntie speelt mede een rol bij dit advies. Hierbij is aansluiten bij het project (in opstartfase) vanuit het Breed Informatiestroomlijn Overleg (BIO) gewenst. Het BIO heeft directe aansluiting op het concernbrede fraudelandschap (FDO, FPO en de [redacted].
[23] Waaronder bredere implementatie van de praktijk bij Toeslagen van weging van een informatieverzoek om vervolgens bij gerede twijfel een (verder te verwerken) signaal op te voeren.
[24] Denk aan opslag in en distributie vanuit datafundamenten ipv handmatig overzetten naar (5+)systemen zoals nu gebeurt.

- logging- en monitoring van het gegevensgebruik.

In meer algemene (organisatorische) zin wordt geadviseerd het functionele herontwerp te doen vanuit het perspectief van de geplande doorontwikkeling/migratie van soortgelijke voorzieningen (RTVs[25]) zoals het OPO-tool, het Informatiesjabloon, IVT en Inzicht en indachtig ontwikkeling op het gebied van het hiervoor al genoemde BIO en een recent memo voor de STAS over fraudemeldpunten.

De voorgestelde migratie/herontwerp is (nog) niet opgenomen in het IV-portfolio[26]. Daarom is bij de oplevering van de 1.0 versie van de PIA een aantal voorlopige verbetermaatregelen op de huidige opzet van FSV opgenomen, die hieronder in voorkomend geval met de actuele stand per 1/11/2019 is beschreven.

1. Het toetsen van de bestaande autorisaties op noodzakelijkheid en actualiteit/geldigheid gevolgd door 'schoning' op basis van de uitkomst van de toetsing.
   @ Op instructie van de ketenvoorzitter GKT is op 24 mei 2019 FSV door wijziging van het toegangspad onbenaderbaar gemaakt en op 27/5 weer beschikbaar gesteld via een alternatief toegangspad na individuele toetsing van de noodzakelijkheid van toegang tot FSV. Het aantal actieve autorisaties is daardoor gedaald van ruim 5000 naar ongeveer 1000. Er is een restrisico dat medewerkers buiten de groep van 1000 na kennisname van de link naar het nieuwe pad alsnog gebruiken. Dit is in de gebruiksvoorwaarden expliciet verboden[27].
2. Het schonen van een aantal jaarlagen (bv jongste signaal over betrokkene is > X jaar).
   @ Uitvoering van schonen staat gepland voor @4 2019. X = 7 jaar.
3. Het aanbrengen van onderscheid tussen een signaal en een informatieverzoek bij verdere verwerking van FSV data in andere informatiesystemen / analyseomgevingen.
4. Een proces- en/of functionele wijziging voor het zo objectief mogelijk vastleggen van het 'gewicht' van een signaal.
5. Implementeren van een uniforme werkwijze[28] om op fiscale relevantie onderzochte informatieverzoeken op te voeren als signaal en deze signalen (verder) te verwerken in plaats van de informatieverzoeken.
6. Het verwijderen/de-activeren (of nader beperken qua gebruikersgroep)van massale en/of integrale exportfunctie(s).
   @ Uitvoering (uitfaseren en inperken bepaalde rollen) staat gepland voor @4 2019. Alleen senior behandelaar kan dan nog exporteren. Deze rol wordt relatief terughoudend uitgeven. (Momenteel nog 105 maal (10% gebruikers)). Nader inperken tot bv. max 2 functionarissen per te onderscheiden bedrijfsonderdelen wordt aanbevolen.
7. Verbeteren van kennis en gebruik van FSV in het bijzonder ten aanzien van de mogelijke privacyrisico's zoals stigmatisering. Hier kan ook worden gedacht aan een Code of Practice/gebruikersinstructie met ethische- en privacy-uitgangspunten, mogelijk in een breder verband dan FSV.

Maak hierbij gebruik van de al aanwezige informatie in het document 180329 F18.045 Feature aanpassingen Dagboek FSV v0.5 en eerder vastgelegde oplossingsmogelijkheden voor herbouw.

[25] RTV: robuuste tijdelijke voorzieningen
[26] Verslag ketentafel GKT van 270619 stelt dat "....Aan een duurzame oplossing wordt op dit moment gewerkt"
[27] Mailbericht aan gebruikers van 25/06 '*autorisatie / toegang tot FSV*'
[28] TSL boekt bijvoorbeeld alle fraudepostbussignalen in BPM en ong. 10% in FSV; MKB FRAUDE EOS boekt alles in FSV, FIOD niets.