



Persoonsgegevens

Team Windows Server

**Belastingdienst Datacenter Services  
Hosting- en Integratiediensten -  
Windows Server**

Laan van Westenenk 494  
Quintax Oost A 4.73  
7334 DS Apeldoorn

Persoonsgegevens

Persoonsgegevens --21-07-2020 10:56:16--Geachte heer [Redacted] Tijdens het onderzoek ter plaatse op 30 jun

[Redacted] @autoriteitpersoonsgegevens.nl>  
[Redacted] @belastingdienst.nl> [Redacted] @belastingdienst.nl> [Redacted] @minfin.nl>  
[Redacted] @minfin.nl>

Datum: 21-07-2020 10:56  
Onderwerp: FSV database ontbrekende bijlagen

Geachte heer [Redacted] Persoonsgegevens

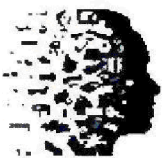
Tijdens het onderzoek ter plaatse op 30 juni jl. is aan ons de FSV applicatie getoond. Op een gegeven moment tijdens het gesprek is ter sprake gekomen dat er in de FSV applicatie ook documenten als bijlagen hingen. We hebben toen ter plekke getest of een bijlage kon worden geopend (ik kan mij herinneren een kopie paspoort) en dit was het geval. Door [Redacted] is toen ook gesteld dat door deze bijlagen de database zou zwaar was, waardoor deze niet op diezelfde dag aan ons meegegeven kon worden.

Na een eerste analyse van de op 6 juli jl. ontvangen FSV database constateren wij dat er geen bijlagen in zitten. Er is wel een tabel getiteld 'Bijlage' maar deze bevat alleen de bestandsnamen van de bijlagen. De bijlagen zijn onderdeel van de FSV database dus daarom verzoek ik u vriendelijk om alsnog ook de bijlagen aan ons aan te leveren, op zo een manier zodat wij de koppeling kunnen maken tussen de unieke bijlage-ID en de aangeleverde bijlage. Ik verzoek u dit uiterlijk woensdag 29 juli 2020 te doen.

Met vriendelijke groet,

[Redacted] Persoonsgegevens

**Senior juridisch medewerker**



**AUTORITEIT  
PERSOONSgegevens**

Kantoor: 070 8888 500

[Redacted] Persoonsgegevens

Fax: 070 8888 501

53

Persoonsgegevens

**Van:** Persoonsgegevens  
**Verzonden:** donderdag 23 juli 2020 09:50  
**Aan:** Persoonsgegevens @belastingdienst.nl  
**CC:** Persoonsgegevens  
**Onderwerp:** RE: Betr: FSV database ontbrekende bijlagen

Geachte heer Persoonsgegevens

Dank u voor uw reactie. Aan ons is toegezegd dat wij de bijlagen zouden ontvangen die in de FSV applicatie zouden zijn opgeslagen. Tijdens het onderzoek ter plaatse bleek ook dat soms/vaak documenten buiten de applicatie werden opgeslagen, bijvoorbeeld in Eldoc. De documenten die op andere locaties of in andere applicaties zijn opgeslagen vallen buiten het informatieverzoek van de Autoriteit Persoonsgegevens. Ik verzoek u daarom vriendelijk om, ook gezien de door mij gestelde deadline, de 36 gig aan documenten in de map "Bijlage" te verstrekken. Kan dit via de Bestandenpostbus? (de uploadcapaciteit van mijn account is ongelimiteerd). Als u wilt overleggen met een van onze technologen, dan kan dit uiteraard. Hieronder vind u mijn contactgegevens.

Met vriendelijke groet,

Persoonsgegevens

Senior juridisch medewerker



AUTORITEIT  
PERSOONSGEGEVENS

Kantoor: 070 8888 500

Persoonsgegevens

Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag

Postadres: Postbus 93374, 2509 AJ Den Haag

[www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl)

**'Privacy gaat iedereen wat aan'**

De privacywet (AVG) zorgt voor meer grip op persoonsgegevens. Weten wat de privacywet voor jou betekent? Kijk op [www.hulpbijprivacy.nl](http://www.hulpbijprivacy.nl).

**Van:** Persoonsgegevens @belastingdienst.nl <Persoonsgegevens@belastingdienst.nl>

**Verzonden:** woensdag 22 juli 2020 11:00

**Aan:** Persoonsgegevens @autoriteitpersoonsgegevens.nl

**CC:** Persoonsgegevens @minfin.nl; Persoonsgegevens

Persoonsgegevens@minfin.nl

**Onderwerp:** Betr: FSV database ontbrekende bijlagen

Hoi Persoonsgegevens

Ik heb de vraag doorgezet. De inhoudelijke werking van de applicatie is mij niet bekend, de map "bijlage" is wel terug te vinden op de server en is rond de 60gig.  
Mogelijk is dat alles maar het kan ook zijn dat bijlage verwijzen naar andere locaties of applicaties.

54



Persoonsgegevens

**Van:** Persoonsgegevens  
**Verzonden:** donderdag 23 juli 2020 11:49  
**Aan:** Persoonsgegevens@minfin.nl  
**CC:** Persoonsgegevens  
**Onderwerp:** Guidance ondersteuning intern toezicht totstandkoming nieuwe fraudesignalen applicatie

Geachte mevrouw Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) doet op dit moment onderzoek naar de FSV applicatie. De brief van de AP gericht aan de Staatssecretarissen van Financiën over het onderzoek staat inmiddels ook online:

<https://www.rijksoverheid.nl/documenten/kamerstukken/2020/07/10/aankondiging-onderzoek-ap-naar-fsv>

Op de tweede pagina van deze brief is verwoord dat de AP naast het onderzoek (dat terugkijkt) ook door middel van guidance de uitvoering van het interne toezicht op de totstandkoming van de toekomstige applicatie met vermoedelijke fraudesignalen wil ondersteunen. Persoonsgegevens heeft mij recent gevraagd hoe de AP hier invulling aan wil geven. Inmiddels heb ik hierover contact gehad met mijn collega Persoonsgegevens (in de cc) en met hem afgesproken dat hij in de week van 10 augustus contact zal opnemen met de Persoonsgegevens hierover. Het traject van het geven van guidance zal door Persoonsgegevens worden verzorgd en zal los staan van het onderzoek.

Ik hoop u hiermee voldoende geïnformeerd te hebben.

Met vriendelijke groet,

Persoonsgegevens

Senior juridisch medewerker



AUTORITEIT  
PERSOONSgegevens

Telefoon: 070 8888 500

Persoonsgegevens

Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag

Postadres: Postbus 93374, 2509 AJ Den Haag

[www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl)

**'Privacy gaat iedereen wat aan'**

De privacywet (AVG) zorgt voor meer grip op persoonsgegevens. Weten wat de privacywet voor jou betekent? Kijk op [www.hulpbijprivacy.nl](http://www.hulpbijprivacy.nl).

55

Persoonsgegevens

**Van:** Persoonsgegevens@minfin.nl>  
**Verzonden:** vrijdag 24 juli 2020 18:09  
**Aan:** Persoonsgegevens  
**Onderwerp:** onderzoek AP naar FSV

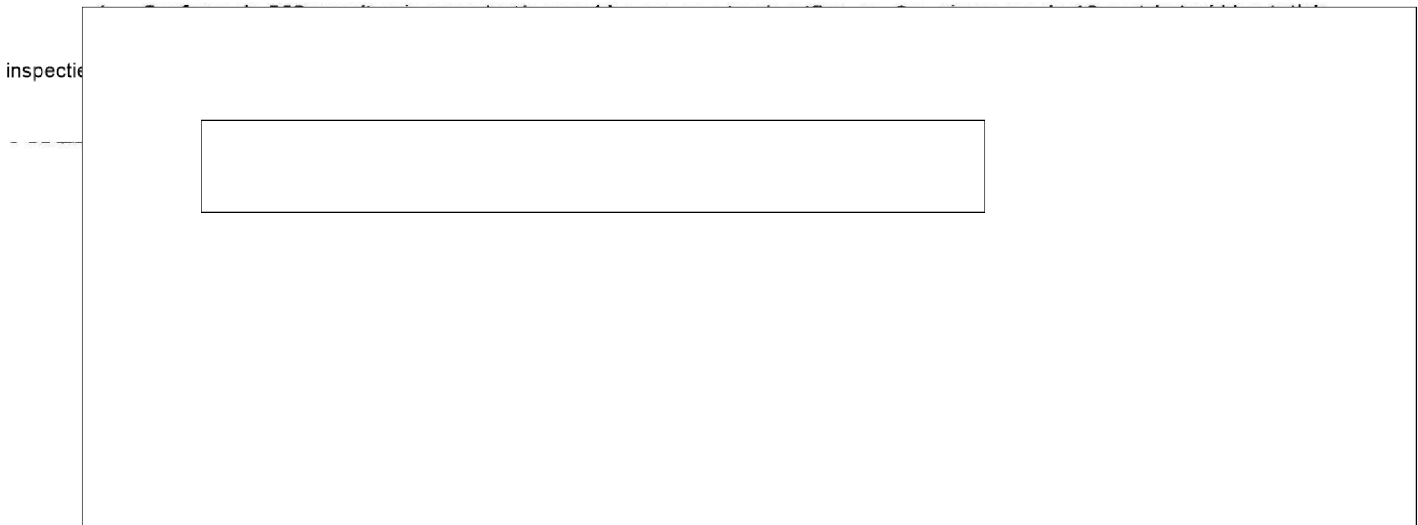
Geachte mevrouw Persoonsgegevens

Hierbij een korte terugkoppeling inzake de gevraagde documenten.

Ontbrekende (vierde) bestand :  
Het bestand is op 24 juli 2020 ge-upload naar de bestandenpostbus

Acties door de heer Persoonsgegevens  
Het exacte moment van uitschakelen FSV zichtbaar in logging: op 24 juli 2020 zijn twee bestanden met gevraagde informatie naar bestandenpostbus gestuurd.

Onderstaande vragen zijn nog onbeantwoord gebleven. De reden hiervan is dat de reacties van de collega's geen voldoende antwoord op de vragen van de AP zijn. De heer Persoonsgegevens zal maandag nogmaals bij de collega's aandringen op beantwoording van de vragen. De heer Persoonsgegevens zal hierover contact met u opnemen.



- lijst met opgevraagde documenten
- Document 4 en 5: gecombineerd
  - Document 6 en 8: identiek
  - Document 11: ontbreekt, nog niet ontvangen
  - Document 12: ontbreekt, nog niet ontvangen
  - Document 14: ontbreekt,
  - Document 19: ontbreekt
  - Document 20-22: ontbreken, nog niet ontvangen
  - Document 35: reeds toegevoegd

Bijlagen bij applicatie FSV  
De heer Persoonsgegevens zal aanstaande maandag contact opnemen met de technoloog van AP waarmee hij eerder contact heeft gehad om het bestand met de bijlagen via bestandenpostbus te sturen. Hij heeft technische ondersteuning nodig vanuit de AP. Het bestand is 36Gigabyte groot en bij de vorige upload van de database (die veel kleiner is), liep de upload regelmatig vast en moest het verzenden opnieuw gebeuren.

Te interviewen persoon  
Naar verwachting wordt begin volgende week bekend welke collega de vragen van de AP over de logging kan beantwoorden. De heer Persoonsgegevens zal met u contact opnemen om een afspraak te plannen.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Persoonsgegevens

**Ministerie van Financiën**  
**Directoraat-Generaal Belastingdienst**  
**Concerndirectie Informatievoorziening en databeheersing**  
Korte Voorhout 7 | 2511 CW | DEN HAAG  
Postbus 20201 | 2500 EE | DEN HAAG

Persoonsgegevens

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

36

7





FW: GRAAG SPOED - GRAAG ADVIES \_ FW: Advies inzake

Persoonsgegevens

Persoonsgegevens 24-03-2020 23:50 Aan: Persoonsgegevens@belastingdienst.nl'

Van: Persoonsgegevens@minfin.nl&gt;

Aan: Persoonsgegevens@belastingdienst.nl&gt;

Persoonsgegevens

Concerndirectie IV&Data beheersing  
 Directoraat Generaal Belastingdienst  
 Ministerie van Financiën

Persoonsgegevens

Van: Persoonsgegevens@minfin.nl&gt;

Verzonden: woensdag 26 februari 2020 17:44

Aan: Persoonsgegevens@minfin.nl&gt;

CC: Persoonsgegevens@minfin.nl, Persoonsgegevens@belastingdienst.nl'

Persoonsgegevens@belastingdienst.nl&gt; Persoonsgegevens@belastingdienst.nl Persoonsgegevens

Persoonsgegevens@minfin.nl&gt;

**Onderwerp:** RE: GRAAG SPOED - GRAAG ADVIES \_ FW: Advies inzake FSV

Persoonsgegevens

Hierbij mijn advies over de GEB (PIA) FSV, versie 1.2.

De conclusie van het rapport is dat de huidige opzet van FSV geen goede aansluiting meer heeft op de verwerkingsbeginselen van art. 5 AVG.

Gelet op de in de PIA beschreven bevindingen en risico's acht ik deze conclusie aannemelijk.

In verband daarmee beveel ik aan om de persoonsgegevens niet, of niet langer op deze wijze te verwerken zolang de maatregelen uit het rapport niet volledig zijn uitgevoerd, of anderszins de verwerking van persoonsgegevens in overeenstemming is gebracht met de AVG. Hierbij heb ik ook het volgende in aanmerking genomen.

- De verwerking betreft volgens de PIA ook bijzondere en strafrechtelijke persoonsgegevens. Het staat buiten twijfel dat het verwerken van zulke gevoelige gegevens alleen mag plaatsvinden als dat verantwoord is. Dat is naar ik begrijp uit de PIA nu niet het geval. De juridische beoordeling in de PIA in het licht van de AVG behoeft overigens nog nadere uitwerking.
- De verwerking van persoonsgegevens voor de in de PIA omschreven doeleinden, heb ik als zodanig nog niet aangetroffen in het register van verwerkingen van persoonsgegevens van het ministerie van Financiën. Uit artikel 30, eerste lid, AVG volgt dat de verwerkingsactiviteiten die onder de verantwoordelijkheid van de verwerkingsverantwoordelijke plaatsvinden, in een register worden bijgehouden. Het Privacybeleid Financiën zegt hierover bovendien het volgende.  
*"Het Verwerkingsregister heeft als doel een overzicht van de verwerkingsactiviteiten te verschaffen, met het oog op de uitoefening van het toezicht door de FG en de AP. Het Verwerkingsregister bevat informatie over de verwerkingen van persoonsgegevens om aantoonbaar te maken dat aan de verplichtingen uit de AVG wordt voldaan. Het register verschaft een integraal, eenduidig en betrouwbaar beeld wie voor welke verwerking verantwoordelijk is. (...)"*
- Niet duidelijk is hoe de verantwoordelijkheid voor de naleving van de AVG en het privacybeleid binnen het ministerie wordt opgepakt en uitgevoerd. De verantwoordelijkheid lijkt (te) versnipperd. Dit moet worden opgelost. In de PIA is daarover het volgende gesteld:  
*"De (algemeen) directeur(en) MKB, Toeslagen, PDB, FIOD en Douane zijn als gemandateerd verwerkingsverantwoordelijken aangewezen voor de respectievelijke wettelijke taken."*
- Op dit moment is voor mij onvoldoende duidelijk of aan de vereisten is voldaan rond transparantie richting de betrokkene over de (eventuele) verwerking van hun gegevens. Dit zou nader moeten

worden uitgezocht.

- Op basis van het privacybeleid Financiën moet er door de lijnmanager die het betreft aantoonbaar (via een Plan van Aanpak) opvolging worden gegeven aan de aanbevelingen/verbetervoorstellen uit de PIA.
- De betrokkenheid van de *privacy officer* moet geborgd worden. Dit in verband met haar in het privacybeleid vastgelegde taak: "kwaliteitsborging ten aanzien van DPIA's".

Mijn advies aan de Belastingdienst is om de persoonsgegevens in FSV niet (langer) te verwerken zolang de maatregelen uit het rapport niet volledig zijn uitgevoerd, en om bovenstaande punten z.s.m. te herstellen.

Groet,

Persoonsgegevens

**Van:** Persoonsgegevens  
**Verzonden:** woensdag 26 februari 2020 10:26  
**Aan:** Persoonsgegevens  
**CC:** Persoonsgegevens@belastingdienst.nl; Persoonsgegevens@belastingdienst.nl  
**Onderwerp:** GRAAG SPOED - GRAAG ADVIES \_ FW: Advies inzake FSV  
**Urgentie:** Hoog

Hoi Persoonsgegevens

Graag met spoed advies over bijgevoegde geb/dpia FSV.  
We spraken hier eerder over.

Er zijn inmiddels informele bevindingen opgesteld door de collega's van IV&D; zie hieronder.

dank,  
Met vriendelijke groet,

Persoonsgegevens

**Ministerie van Financiën**  
**Directoraat-Generaal Belastingdienst**  
**Concerndirectie Informatievoorziening en databeheersing**  
Korte Voorhout 7 | 2511 CW | DEN HAAG  
Postbus 20201 | 2500 EE | DEN HAAG

Persoonsgegevens

**Van:** Persoonsgegevens@belastingdienst.nl; Persoonsgegevens@belastingdienst.nl  
**Verzonden:** donderdag 20 februari 2020 21:31  
**Aan:** Persoonsgegevens@minfin.nl  
**CC:** Persoonsgegevens@minfin.nl; Persoonsgegevens@minfin.nl; Persoonsgegevens@minfin.nl; Persoonsgegevens@minfin.nl;  
**Onderwerp:** Re: Advies inzake FSV

Hallo Persoonsgegevens

Even voor de volledigheid:

- de Pia heeft versienummer 1.2. Kan concept zijn, maar heeft dan de schijn tegen
- als de Pia nog in concept is en in de Pia staan de concept bevindingen, dan nog heeft de directeur nu een verwerking in de lucht die op z'n minst dubieus te noemen is. Het aanpassen van de Pia maakt de verwerking niet automatisch legitiem. Tenzij natuurlijk de huidige Pia de werkelijkheid geweld aandoet. Maar zelfs in dat geval zou ik mij als directeur zorgen maken over deze specifieke verwerking

Ik vul mijn advies dan ook aan met de aanbeveling om naast het stoppen met de verwerking, de Pia af te ronden. Vervolgens op basis van de uitkomsten te bepalen of de verwerking überhaupt doorgang kan vinden dan wel de daarin beschreven noodzakelijk maatregelen eerst uitgevoerd te hebben voordat de verwerking weer gestart wordt.

Met vriendelijke groet,

Persoonsgegevens

Concerndirectie IV & Databeheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën

Persoonsgegevens

Op 20 feb. 2020 om 21:06 heeft Persoonsgegevens [@minfin.nl](mailto: @minfin.nl) het volgende geschreven:

Allen

Persoonsgegevens gesproken.

De PIA die er nu ligt is een concept versie - er is, of er moet nog een definitieve versie opgeleverd worden die voorgelegd moet worden. Graag morgen even contact met Persoonsgegevens Persoonsgegevens of er iets in zijn workflow nog zit, zo ja, deze eruit halen en zorgen dat we zelf eerst de PIA beoordelen en zonodig eerst laten aanpassen.

Tevens zal ik morgen de eigenaar resp de directies, die FSV gebruiken, vragen om terstond te rapporteren op de maatregelen van toegang, gebruik excel en schonen oude data.

Het advies om de applicatie te herontwerpen, ook op basis van de principes van ADP, moeten we ook opvolgen. De beoordeling of de toepassing dan nu wel of niet binnen de AVG vereisten valt, wil ik nemen na beoordeling van de PIA door de FG. NB. Het is een signaleringssysteem, waarna een reguliere controle volgt. Er is in die zin geen indicatie op basis van dit gebruik dat er sprake is van vervolgschade voor burgers.

Persoonsgegevens

Verzonden met BlackBerry Work



([www.blackberry.com](http://www.blackberry.com))

[...]

Van [Persoonsgegevens] <[redacted]@minfin.nl>  
 Datum: donderdag 20 feb. 2020 7:41 PM  
 Aan: [Persoonsgegevens] <[redacted]@minfin.nl>  
 Kopie: [Persoonsgegevens] <[redacted]@minfin.nl>, [Persoonsgegevens] <[redacted]@minfin.nl>, [Persoonsgegevens] <[redacted]@minfin.nl>, [Persoonsgegevens] <[redacted]@belastingdienst.nl>, [Persoonsgegevens] <[redacted]@belastingdienst.nl>  
 Onderwerp: Advies inzake FSV

[Persoonsgegevens]

Vanmiddag is er in een kleine groep gekeken naar de PIA van de applicatie FSV. Dat heeft een aantal vraagpunten en diverse bevindingen opgeleverd. De meest prangende vragen vanuit het oogpunt van informatiebeveiliging, zie hieronder mail [redacted] heb ik getracht een antwoord op te krijgen van [Persoonsgegevens]

Uit de antwoorden blijkt dat de applicatie FSV op dit moment (donderdag 20 februari 2020, 19:12) nog in de lucht is. Gegeven het feit dat uit de PIA blijkt dat:

- gegevens uit de applicatie middels een dump naar Excel geëxporteerd kunnen worden. Het is niet duidelijk wie de dump ontvangt, wie er verder toegang krijgen tot die dump en wanneer die dump vernietigd wordt;
  - het onduidelijk is of deze verwerking van gegevens op deze manier mag (advies in de PIA is om de applicatie opnieuw te ontwerpen conform de eisen die de AVG stelt);
  - onduidelijk is of de schoning/vernietiging daadwerkelijk plaatsgevonden heeft. Indien niet het geval zijn de gegevens uit 2001 (vanuit migratie voorganger) nog actief aanwezig in het systeem;
  - de applicatie FSV niet voldoet aan de basiseisen die de Belastingdienst stelt aan een applicatie op het gebied van autorisatie en logging en monitoring;
  - de applicatie FSV gegevens levert aan "derden" waarbij het onbekend is of dit toegestaan is;
  - diverse zware gegevensbeschermingsissues en -risico's zijn geconstateerd.
- adviseer ik om:
- de directeur MKB (danwel GO) opdracht te geven de applicatie FSV per omgaande stil te zetten door middel van het ontoegankelijk maken van de applicatie en de bijbehorende database en tevens het veiligstellen van de inhoud tot nadere orde;
  - de directeur MKB opdracht te geven de dumps actief op te sporen en te vernietigen (en te documenteren waar deze dumps zijn aangetroffen);
  - de directeur MKB opdracht te geven om de gevolgschade voor de burger waar mogelijk in kaart te brengen.

Onderstaand de reactie op de PIA zoals hedenavond opgeleverd aan [Persoonsgegevens]

Hallo [Persoonsgegevens]

Na het lezen van de PIA FSV (november 2019) vanuit perspectief "ligt morgen in deze vorm op straat" hebben we de volgende verwonderpunten:

Vragen n.a.v PIA FSV voor MKB:

- Draait deze applicatie nu nog? Antwoord MKB: Ja
- Wie beschikt over mogelijkheid voor systeemdump, wie heeft daar daadwerkelijk gebruik van gemaakt en wat gebeurt er met die dump? Antwoord MKB: onbekend
- Welke externe partijen krijgen nu de (vage)fraude-signalen en op basis van welke wettelijke verplichting? Antwoord MKB: onbekend
- Hebben we inzichtelijk wat er gebeurt met de verouderde gegevens die dus niet gebruikt mogen worden? Antwoord MKB: onbekend

- Heeft de schoning daadwerkelijk plaatsgevonden? Antwoord MKB: onbekend
- Is bekend of de toeslagendossiers zijn "verrijkt" met de informatie vanuit FSV?
- Is bekend in welke dossiers de informatie uit FSV geleid heeft tot rechtsgevolgen (b.v. geen betalingsregeling omdat ooit aangemerkt als "fraudeur")?
- Sprake van "zwarte lijst". Hoe kan een burger daar weet van hebben/van afgevoerd worden?
 

"Enkele van de binnen FSV verwerkte elementen 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."
- PIA beschrijft dat exporteren niet gelogd wordt. Informatie van de data-coördinator is dat er wel gelogd wordt. Wat is nu de werkelijkheid?
- Toegang op basis van Need to know is nu beperkt tot 105 medewerkers. Op basis waarvan is dat aantal tot stand gekomen en waarom waren het er eerst meer dan 5000?
- Toegang tot FSV is volgens PIA geregeld via IMS (dus op basis van een rol). Op pagina 18 wordt het restrisico genoemd dat als een medewerker weet waar de applicatie staat, hij toegang krijgt met als mitigerende maatregel: "dit is volgens de gebruikersvoorwaarden expliciet verboden"..... Eea is totaal in tegenspraak met elkaar (en geen realistische mitigerende maatregel zonder handhaving).
- Er is sprake van het delen van informatie in een gesloten community op CP. Wie bepaalt daar de toegang toe, wie ziet toe op de juistheid van die toegang en wat voor informatie wordt daar gedeeld?

#### Algemeen:

- vragen mbt profilering en subject-gericht toezicht kunnen verwacht worden
- het taalgebruik van de PIA is bij vlagen verwarrend. Veel lange zinnen die –ook na ontleden- niet leesbaar zijn.
- Integriteit van de gegevens is niet geborgd. Medewerkers kunnen elkaars gegevens ongezien muteren
- Logging en monitoring van de handelingen in de applicatie ontbreekt.
- Rechtsgrond "gerechtvaardigd belang" wordt door IV&D betwijfeld.
- Juistheid Doelbinding is op basis van deze pia met onvoldoende zekerheid te bepalen.
- PIA stelt dat rechten van betrokkene ingeperkt kunnen worden op basis van artikel 23 AVG. Dit moet nader bekeken worden alvorens hier een standpunt over in te nemen is.

Genoemde systemen/documenten die opgevraagd kunnen worden (omdat ze genoemd worden in de PIA FSV). Actie voor IV&D is om deze documenten op korte termijn boven water te krijgen.

- PIA Informatieloketten
- PIA IVT
- applicatie OPO-tool
- "Het informatiesjabloon"
- "recent memo aan de Stas inzake Fraudemeldpunt"
- Applicatie "Inzicht"

#### Gevolgen:

Onder de verantwoordelijkheid van een directeur loopt er sinds 2014 (FSV) of zelfs 2001 (PIT) een verwerking waarvan in ieder geval sinds januari 2019 duidelijk is dat er nog onderzoeksvragen met betrekking tot verwerkingsgrondslag, doelbinding en (rest)risico's in zitten. In november 2019 is er een aangescherpte versie van de PIA opgeleverd. Onbekend is welke risico's in de januari-versie genoemd zijn.

Persoonsgegevens

Persoonsgegevens

*Concerndirectie IV&Data-beheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën*

Persoonsgegevens

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

De Belastingdienst stelt e-mail niet open voor aanvragen, aangiften, bezwaarschriften, verzoeken, klachten, ingebrekestellingen en soortgelijke formele berichten.

Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten waarvoor de fiscale geheimhoudingsplicht geldt. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te verwijderen en de afzender te informeren.

The Dutch Tax and Customs Administration does not accept filings, requests, appeals, complaints, notices of default or similar formal notices, sent by email.

This message is solely intended for the addressee. It may contain information that is confidential and legally privileged. If you are not the intended recipient please delete this message and notify the sender.







FW: Geactualiseerde [Redacted] Persoonsgegevens 24-03-2020

05:53 Aan: [Redacted]@belastingdienst.nl

Van: [Redacted] Persoonsgegevens @minfin.nl>

Aan: [Redacted] Persoonsgegevens @belastingdienst.nl>

1 Attachment



20190121 GEB FSV v 1.2 herijking nov 2019.pdf

[Redacted] Persoonsgegevens

Concerndirectie IV&Data beheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën

[Redacted] Persoonsgegevens

Van: [Redacted] Persoonsgegevens @minfin.nl>

Verzonden: donderdag 20 februari 2020 14:20

Aan: [Redacted] Persoonsgegevens @minfin.nl>

Onderwerp: FW: Geactualiseerde PIA/GEB FSV

Van: [Redacted] Persoonsgegevens @minfin.nl>

Verzonden: donderdag 20 februari 2020 14:13

Aan: [Redacted] Persoonsgegevens @minfin.nl>

Onderwerp: FW: Geactualiseerde PIA/GEB FSV

Beste [Redacted] Persoonsgegevens

Hierbij de versie uit nov 2019.

Vriendelijke groet,

[Redacted] Persoonsgegevens

**Ministerie van Financiën**

**Directie Communicatie**

Korte Voorhout 7 | 2511 CW | Den Haag

Postbus 20201 | 2500 EE | Den Haag

[Redacted] Persoonsgegevens

Van: [Redacted] Persoonsgegevens @belastingdienst.nl | [Redacted] Persoonsgegevens @belastingdienst.nl>

Verzonden: donderdag 20 februari 2020 12:54

Aan: @minfin.nl>

Onderwerp: Geactualiseerde PIA/GEB FSV

Beste

Hierbij stuur ik je de in november 2019 geactualiseerde versie van de GEB FSV. De actualisatie is in het bijzonder toegepast op par. 17: maatregelen.

*(Zie het bijgevoegde bestand: 20190121 GEB FSV v 1.2 herijking nov 2019.pdf)*

Met vriendelijke groet, Kind Regards,

Team Juridisch Advies Gegevens  
Email: CAP Juridisch Advies\_Postbus

.....  
Team Quality Assurance  
Belastingdienst/ Centrale Administratieve Processen  
John F. Kennedylaan 8 | 7314 PS | Apeldoorn |  
WBC- gebouw   
Postbus 1254 | 7301 BM | Apeldoorn

-----  
De Belastingdienst stelt e-mail niet open voor aanvragen, aangiften, bezwaarschriften, verzoeken, klachten, ingebrekestellingen en soortgelijke formele berichten.  
Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten waarvoor de fiscale geheimhoudingsplicht geldt. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te verwijderen en de afzender te informeren.

The Dutch Tax and Customs Administration does not accept filings, requests, appeals, complaints, notices of default or similar formal notices, sent by email.  
This message is solely intended for the addressee. It may contain information that is confidential and legally privileged. If you are not the intended recipient please delete this message and notify the sender.

-----  
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.  
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

7



FW: Geactualiseerde [Redacted] Persoonsgegevens 24-03-2020

05:53 Aan: [Redacted]@belastingdienst.nl  
Van: [Redacted] Persoonsgegevens @minfin.nl>  
Aan: [Redacted]@belastingdienst.nl, [Redacted]@belastingdienst.nl

1 Attachment



20190121 GEB FSV v 1.2 herijking nov 2019.pdf

[Redacted] Persoonsgegevens

Concerndirectie IV&Data beheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën

[Redacted] Persoonsgegevens

Van: [Redacted] Persoonsgegevens @minfin.nl>

Verzonden: donderdag 20 februari 2020 14:20

Aan: [Redacted] Persoonsgegevens @minfin.nl>

Onderwerp: FW: Geactualiseerde PIA/GEB FSV

Van: [Redacted] Persoonsgegevens @minfin.nl>

Verzonden: donderdag 20 februari 2020 14:13

Aan: [Redacted] Persoonsgegevens @minfin.nl>

Onderwerp: FW: Geactualiseerde PIA/GEB FSV

Beste [Redacted] Persoonsgegevens

Hierbij de versie uit nov 2019.

Vriendelijke groet,

[Redacted] Persoonsgegevens

Ministerie van Financiën  
Directie Communicatie  
Korte Voorhout 7 | 2511 CW | Den Haag  
Postbus 20201 | 2500 EE | Den Haag

[Redacted] Persoonsgegevens

Van: [Redacted]@belastingdienst.nl, [Redacted]@belastingdienst.nl

Verzonden: donderdag 20 februari 2020 12:54

Aan: @minfin.nl>

Onderwerp: Geactualiseerde PIA/GEB FSV

Beste

Hierbij stuur ik je de in november 2019 geactualiseerde versie van de GEB FSV. De actualisatie is in het bijzonder toegepast op par. 17: maatregelen.

*(Zie het bijgevoegde bestand: 20190121 GEB FSV v 1.2 herijking nov 2019.pdf)*

Met vriendelijke groet, Kind Regards,

Team Juridisch Advies Gegevens  
Email: CAP Juridisch Advies\_Postbus

.....  
Team Quality Assurance  
Belastingdienst/ Centrale Administratieve Processen  
John F. Kennedylaan 8 | 7314 PS | Apeldoorn |  
WBC- gebouw   
Postbus 1254 | 7301 BM | Apeldoorn

---

De Belastingdienst stelt e-mail niet open voor aanvragen, aangiften, bezwaarschriften, verzoeken, klachten, ingebrekestellingen en soortgelijke formele berichten.  
Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten waarvoor de fiscale geheimhoudingsplicht geldt. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te verwijderen en de afzender te informeren.

The Dutch Tax and Customs Administration does not accept filings, requests, appeals, complaints, notices of default or similar formal notices, sent by email.  
This message is solely intended for the addressee. It may contain information that is confidential and legally privileged. If you are not the intended recipient please delete this message and notify the sender.

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.  
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.



7



FW: 20190121 GEB FSV v 1.2 herijking nov 2019.pdf

Persoonsgegevens

Van: [Redacted] 24-03-2020 23:44 Aan: [Redacted]@belastingdienst.nl

Van: [Redacted] Persoonsgegevens @minfin.nl>

Aan: [Redacted]@belastingdienst.nl Persoonsgegevens@belastingdienst.nl>

1 Attachment



20190121 GEB FSV v 1.2 herijking nov 2019.pdf

Persoonsgegevens

Concerndirectie IV&Databeheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën

Persoonsgegevens

Van: [Redacted] Persoonsgegevens @minfin.nl>

Verzonden: donderdag 20 februari 2020 16:18

Aan: [Redacted] Persoonsgegevens @minfin.nl>

Onderwerp: 20190121 GEB FSV v 1.2 herijking nov 2019.pdf

Hoi,

Hierbij de recentste GEB/DPIA van nov 2019.

Met vriendelijke groet,

Persoonsgegevens

Ministerie van Financiën  
Directoraat-Generaal Belastingdienst  
Concerndirectie Informatievoorziening en databeheersing  
Korte Voorhout 7 | 2511 CW | DEN HAAG  
Postbus 20201 | 2500 EE | DEN HAAG

Persoonsgegevens

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.  
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

bylage 5





FW: Advies inzake FSV [Redacted] Persoonsgegevens 24-03-2020 05:52 Aan:

[Redacted] Persoonsgegevens@belastingdienst.nl'

Van: [Redacted] Persoonsgegevens @minfin.nl>

Aan: [Redacted] Persoonsgegevens@belastingdienst.nl' [Redacted] Persoonsgegevens@belastingdienst.nl>

[Redacted] Persoonsgegevens

Concerndirectie IV&Databeheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën

[Redacted] Persoonsgegevens

Van: [Redacted] Persoonsgegevens@belastingdienst.nl' [Redacted] Persoonsgegevens@belastingdienst.nl>

Verzonden: donderdag 20 februari 2020 21:31

Aan: [Redacted] Persoonsgegevens @minfin.nl>

CC: [Redacted] Persoonsgegevens @minfin.nl> [Redacted] Persoonsgegevens

[Redacted] Persoonsgegevens@minfin.nl>; [Redacted] Persoonsgegevens @minfin.nl>;

[Redacted] Persoonsgegevens@belastingdienst.nl

Onderwerp: Re: Advies inzake FSV

Hallo [Redacted] Persoonsgegevens

Even voor de volledigheid:

- de Pia heeft versienummer 1.2. Kan concept zijn, maar heeft dan de schijn tegen
- als de Pia nog in concept is en in de Pia staan de concept bevindingen, dan nog heeft de directeur nu een verwerking in de lucht die op z'n minst dubieus te noemen is. Het aanpassen van de Pia maakt de verwerking niet automatisch legitiem. Tenzij natuurlijk de huidige Pia de werkelijkheid geweld aandoet. Maar zelfs in dat geval zou ik mij als directeur zorgen maken over deze specifieke verwerking

Ik vul mijn advies dan ook aan met de aanbeveling om naast het stoppen met de verwerking, de Pia af te ronden. Vervolgens op basis van de uitkomsten te bepalen of de verwerking überhaupt doorgang kan vinden dan wel de daarin beschreven noodzakelijk maatregelen eerst uitgevoerd te hebben voordat de verwerking weer gestart wordt.

Met vriendelijke groet,

[Redacted] Persoonsgegevens

Concerndirectie IV & Databeheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën

[Redacted] Persoonsgegevens

Op 20 feb. 2020 om 21:06 heeft Persoonsgegevens [minfin.nl](mailto:persoonsgegevens@minfin.nl)> het volgende geschreven:

Allen

Persoonsgegevens even gesproken.

De PIA die er nu ligt is een concept versie - er is, of er moet nog een definitieve versie opgeleverd worden die voorgelegd moet worden. Graag morgen even contact met Persoonsgegevens of er iets in zijn workflow nog zit, zo ja, deze eruit halen en zorgen dat we zelf eerst de PIA beoordelen en zonodig eerst laten aanpassen.

Tevens zal ik morgen de eigenaar resp de directies, die FSV gebruiken, vragen om terstond te rapporteren op de maatregelen van toegang, gebruik excel en schonen oude data.

Het advies om de applicatie te herontwerpen, ook op basis van de principes van ADP, moeten we ook opvolgen. De beoordeling of de toepassing dan nu wel of niet binnen de AVG vereisten valt, wil ik nemen na beoordeling van de PIA door de FG. NB. Het is een signaleringssysteem, waarna een reguliere controle volgt. Er is in die zin geen indicatie op basis van dit gebruik dat er sprake is van vervolgschade voor burgers.

Persoonsgegevens

Verzonden met BlackBerry Work  
([www.blackberry.com](http://www.blackberry.com))

**Van:** Persoonsgegevens [@minfin.nl](mailto:persoonsgegevens@minfin.nl)>  
**Datum:** donderdag 20 feb. 2020 8:20 PM  
**Aan:** Persoonsgegevens [@minfin.nl](mailto:persoonsgegevens@minfin.nl)>  
**Kopie:** Persoonsgegevens [@minfin.nl](mailto:persoonsgegevens@minfin.nl)>, Persoonsgegevens [@minfin.nl](mailto:persoonsgegevens@minfin.nl)>, Persoonsgegevens [@belastingdienst.nl](mailto:persoonsgegevens@belastingdienst.nl)>, Persoonsgegevens [@belastingdienst.nl](mailto:persoonsgegevens@belastingdienst.nl)>  
**Onderwerp:** RE: Advies inzake FSV

Hi Persoonsgegevens

Dank; ik heb Persoonsgegevens geïnformeerd, na overleg met hem morgenochtend, ga ik onderstaande lijn ook doorpakken.

NB. Graag obv inventarisatie ten tijde van AVG traject, bij alle onderdelen navraag doen op de AVG risicovolle applicaties. Ik hoor bv applicatie met naam 'tabbladen' bij Douane, ..

Persoonsgegevens

Verzonden met BlackBerry Work  
([www.blackberry.com](http://www.blackberry.com))

**Van:** Persoonsgegevens [@minfin.nl](mailto:persoonsgegevens@minfin.nl)>

Datum: donderdag 20 feb. 2020 7:41 PM

Aan [Persoonsgegevens]@minfin.nl>

Kopie: [Persoonsgegevens]@minfin.nl>, [Persoonsgegevens]@minfin.nl>, [Persoonsgegevens]@minfin.nl>, [Persoonsgegevens]@belastingdienst.nl>, [Persoonsgegevens]@belastingdienst.nl>

Onderwerp: Advies inzake FSV

[Persoonsgegevens]

Vanmiddag is er in een kleine groep gekeken naar de PIA van de applicatie FSV. Dat heeft een aantal vraagpunten en diverse bevindingen opgeleverd. De meest prangende vragen vanuit het oogpunt van informatiebeveiliging, zie hieronder mail [Persoonsgegevens] ik getracht een antwoord op te krijgen van [Persoonsgegevens]

Uit de antwoorden blijkt dat de applicatie FSV op dit moment (donderdag 20 februari 2020, 19:12) nog in de lucht is. Gegeven het feit dat uit de PIA blijkt dat:

- gegevens uit de applicatie middels een dump naar Excel geëxporteerd kunnen worden. Het is niet duidelijk wie de dump ontvangt, wie er verder toegang krijgen tot die dump en wanneer die dump vernietigd wordt;
- het onduidelijk is of deze verwerking van gegevens op deze manier mag (advies in de PIA is om de applicatie opnieuw te ontwerpen conform de eisen die de AVG stelt);
- onduidelijk is of de schoning/vernietiging daadwerkelijk plaatsgevonden heeft. Indien niet het geval zijn de gegevens uit 2001 (vanuit migratie voorganger) nog actief aanwezig in het systeem;
- de applicatie FSV niet voldoet aan de basiseisen die de Belastingdienst stelt aan een applicatie op het gebied van autorisatie en logging en monitoring;
- de applicatie FSV gegevens levert aan "derden" waarbij het onbekend is of dit toegestaan is;
- diverse zware gegevensbeschermingsissues en -risico's zijn geconstateerd.

adviseer ik om:

- de directeur MKB (danwel GO) opdracht te geven de applicatie FSV per omgaande stil te zetten door middel van het ontoegankelijk maken van de applicatie en de bijbehorende database en tevens het veiligstellen van de inhoud tot nadere orde;
- de directeur MKB opdracht te geven de dumps actief op te sporen en te vernietigen (en te documenteren waar deze dumps zijn aangetroffen);
- de directeur MKB opdracht te geven om de gevolgschade voor de burger waar mogelijk in kaart te brengen.

Onderstaand de reactie op de PIA zoals hedenavond opgeleverd aan [Persoonsgegevens]

Hallo [Persoonsgegevens]

Na het lezen van de PIA FSV (november 2019) vanuit perspectief "ligt morgen in deze vorm op straat" hebben we de volgende verwonderpunten:

Vragen n.a.v PIA FSV voor MKB:

- Draait deze applicatie nu nog? Antwoord MKB: Ja
- Wie beschikt over mogelijkheid voor systeemdump, wie heeft daar daadwerkelijk gebruik van gemaakt en wat gebeurt er met die dump? Antwoord MKB: onbekend
- Welke externe partijen krijgen nu de (vage)fraude-signalen en op basis van welke wettelijke verplichting? Antwoord MKB: onbekend
- Hebben we inzichtelijk wat er gebeurt met de verouderde gegevens die dus niet gebruikt mogen worden? Antwoord MKB: onbekend
- Heeft de schoning daadwerkelijk plaatsgevonden? Antwoord MKB: onbekend
- Is bekend of de toeslagendossiers zijn "verrijkt" met de informatie vanuit FSV?
- Is bekend in welke dossiers de informatie uit FSV geleid heeft tot rechtsgevolgen (b.v. geen betalingsregeling omdat ooit aangemerkt als "fraudeur")?
- Sprake van "zwarte lijst". Hoe kan een burger daar weet van hebben/van afgevoerd worden?

"Enkele van de binnen FSV verwerkte elementen en 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."
- PIA beschrijft dat exporteren niet gelogd wordt. Informatie van de data-coördinator is dat er wel gelogd wordt. Wat is nu de werkelijkheid?
- Toegang op basis van Need to know is nu beperkt tot 105 medewerkers. Op basis waarvan is dat aantal tot stand gekomen en waarom waren het er eerst meer dan 5000?
- Toegang tot FSV is volgens PIA geregeld via IMS (dus op basis van een rol). Op pagina 18 wordt het restrisico genoemd dat als een medewerker weet waar de applicatie staat, hij toegang krijgt met als mitigerende maatregel: "dit is volgens de gebruikersvoorwaarden expliciet verboden"..... Eea is totaal in tegenspraak met elkaar (en geen realistische mitigerende maatregel zonder handhaving).
- Er is sprake van het delen van informatie in een gesloten community op CP. Wie bepaalt daar de toegang toe, wie ziet toe op de juistheid van die toegang en wat voor informatie wordt daar gedeeld?

**Algemeen:**

- vragen mbt profilering en subject-gericht toezicht kunnen verwacht worden
- het taalgebruik van de PIA is bij vlagen verwarrend. Veel lange zinnen die -ook na ontleden- niet leesbaar zijn.
- Integriteit van de gegevens is niet geborgd. Medewerkers kunnen elkaars gegevens ongezien muteren
- Logging en monitoring van de handelingen in de applicatie ontbreekt.
- Rechtsgrond "gerechtvaardigd belang" wordt door IV&D betwijfeld.
- Juistheid Doelbinding is op basis van deze pia met onvoldoende zekerheid te bepalen.
- PIA stelt dat rechten van betrokkene ingeperkt worden op basis van artikel 23 AVG. Dit moet nader bekeken worden alvorens hier een standpunt over in te nemen is.

Genoemde systemen/documenten die opgevraagd kunnen worden (omdat ze genoemd worden in de PIA FSV). Actie voor IV&D is om deze documenten op korte termijn boven water te krijgen.

- PIA Informatieloketten
- PIA IVT
- applicatie OPO-tool
- "Het informatiesjabloon"
- "recent memo aan de Stas inzake Fraudemeldpunt"
- Applicatie "Inzicht"

**Gevolgen:**

Onder de verantwoordelijkheid van een directeur loopt er sinds 2014 (FSV) of zelfs 2001 (PIT) een verwerking waarvan in ieder geval sinds januari 2019 duidelijk is dat er nog onderzoeksvragen met betrekking tot verwerkingsgrondslag, doelbinding en (rest)risico's in zitten. In november 2019 is er een aangescherpte versie van de PIA opgeleverd. Onbekend is welke risico's in de januari-versie genoemd zijn.

Persoonsgegevens

*Concerndirectie IV&Data beheersing  
 Directoraat Generaal Belastingdienst  
 Ministerie van Financiën*

Persoonsgegevens

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan

u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

De Belastingdienst stelt e-mail niet open voor aanvragen, aangiften, bezwaarschriften, verzoeken, klachten, ingebrekestellingen en soortgelijke formele berichten.

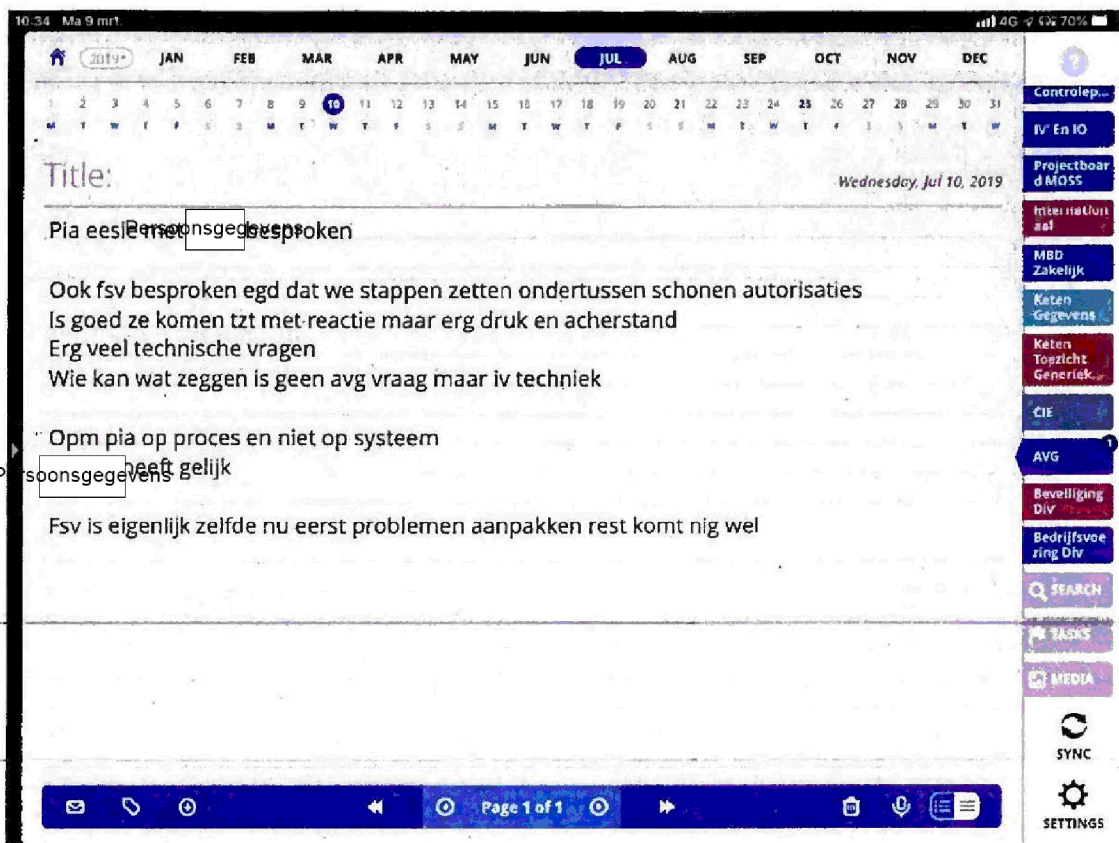
Dit bericht is uitsluitend bestemd voor de geadresseerde. Het bericht kan vertrouwelijke informatie bevatten waarvoor de fiscale geheimhoudingsplicht geldt. Als u dit bericht per abuis hebt ontvangen, wordt u verzocht het te verwijderen en de afzender te informeren.

The Dutch Tax and Customs Administration does not accept filings, requests, appeals, complaints, notices of default or similar formal notices, sent by email.

This message is solely intended for the addressee. It may contain information that is confidential and legally privileged. If you are not the intended recipient please delete this message and notify the sender.







Schermsprint iPad medewerker MKB 10 juli 2019

b̄y lage. 7

7





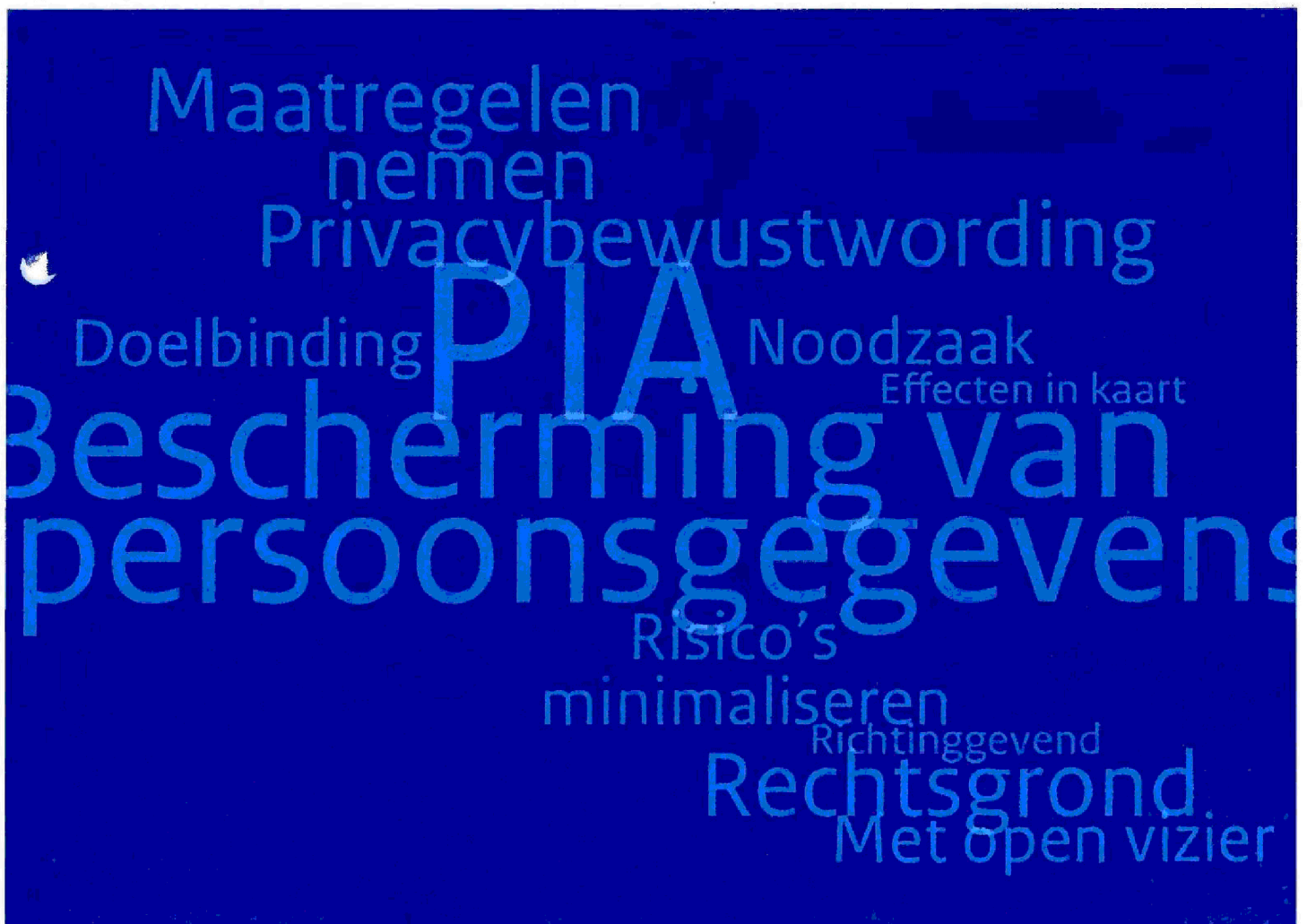
## Gegevensbeschermingseffectbeoordeling (PIA)

# FSV (Fraude Signalering Voorziening)

Ministerie van Financiën

Belastingdienst/Midden- en KleinBedrijf (MKB)

Utrecht, 21 januari 2019



Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: de Minister van Financiën, namens deze,

Advies functionaris voor gegevensbescherming: Selecteer/typ datum .

Naam:

Advies CIO: Selecteer/typ datum

Naam:

## Gegevensbeschermings- effectbeoordeling (GEB/PIA)

**Ministerie van Financiën**  
**Belastingdienst/Midden- en KleinBedrijf (MKB)**

### Contact:

Ministerie van Financiën, directie Belastingdienst/CAP  
Cluster Gegevens  
Unit Inwinnen en Verstrekken van Gegevens

Team Juridisch Advies Gegevens

Persoonsgegevens

Persoonsgegevens@belastingdienst.nl

### Materiedeskundigen:

Persoonsgegevens

Versie: 1.0 November 2018

## Inhoudsopgave

A. Beschrijving kenmerken gegevensverwerkingen .....	5
1.    Voorstel .....	5
2.    Persoonsgegevens .....	6
3.    Gegevensverwerkingen .....	6
4.    Verwerkingsdoeleinden .....	7
5.    Betrokken partijen .....	8
6.    Belangen bij de gegevensverwerking .....	8
7.    Verwerkingslocaties .....	9
8.    Techniek en methode van gegevensverwerking .....	9
9.    Juridisch en beleidsmatig kader .....	11
10.   Bewaartermijnen .....	11
B: Beoordeling rechtmatigheid gegevensverwerkingen.....	12
11.   Rechtsgrond .....	12
12.   Bijzondere persoonsgegevens .....	12
13.   Doelbinding .....	14
14.   Noodzaak en evenredigheid .....	16
15.   Rechten van de betrokkene .....	17
C. Beschrijving en beoordeling risico's voor de betrokkenen .....	18
16.   Risico's.....	18
D. Beschrijving voorgenomen maatregelen .....	19
17.   Maatregelen.....	20



## A. Beschrijving kenmerken gegevensverwerkingen

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

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

### 1. Voorstel

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

Aanleiding voor deze GEB 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 GEB 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<sup>1</sup>. 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<sup>2</sup>. 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 GEB op een bestaande gegevensverwerking vanuit een eerdere risicoschatting in de voornoemde GEB Informatieloketten. FSV kent vier hoofd-verwerkingsvormen (tabbladen) die waar nodig onderscheiden beoordeeld zullen worden in deze PIA. Dit betreft:

1. Aanmaken/bewerken aangiftefraude<sup>3</sup>.
2. Aanmaken/behandelen informatieverzoek.
3. Aanmaken/behandelen Tip/Klikmelding.
4. Aanmaken/behandelen project.

<sup>1</sup> 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.

<sup>2</sup> Er is een directe relatie met de facultatieve GEB Informatieloketten van mei 2018.

<sup>3</sup> 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.

## 2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

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);
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 bedrijfs onderdeel een verschillend gebruik gemaakt (zie 5. Betrokken partijen) en zijn er binnen bedrijfs onderdelen verschillen in het gebruik. Bijvoorbeeld enkele MKB-EOS-teams die alleen algemene signaal informatie 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 **registreren**. 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 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<sup>4</sup>.

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 '**steemdump**' via de excel-exportfunctie.

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

#### 4. Verwerkingsdoeleinden

**Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.**

Voor het uitvoeren van zijn taken op het gebied van uitvoering van heffing en inning, waaronder risicovinding<sup>5</sup>, 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

<sup>4</sup> 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.

<sup>5</sup> bv. OB-carrouselfraude, Combiteam Aanpak Facilitators (CAF)

(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. renseignements.

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<sup>6</sup>.

## 5. Betrokken partijen

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

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

De (algemeen) directeur(en) MKB, Toeslagen, PDB, FIOD en Douane zijn als gedelegeerd 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.**

<sup>6</sup> Voor MKB: zie hiervoor de afgeronde GEB op de informatieloketten.



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<sup>7</sup>. 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.

## 8. Techniek en methode van gegevensverwerking

**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 data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.**

<sup>7</sup> De (voormalige) AntiFraudeBox (AFB) is om deze reden destijds geautoriseerd. Idem EHI.

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 carousel-fraude). 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<sup>9</sup>. Enkele van de binnen FSV verwerkte elementen<sup>9</sup> 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<sup>10</sup>. 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 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.**

Hoewel procesmatig onderkend<sup>11</sup> 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.

---

<sup>8</sup> Standpunt/beslissing DT BD, verslag 7 juni 2018.

<sup>9</sup> Zoals risico-scores of mogelijk subjectieve waarderingen uit andere processen: negatieve-norm OB, prioriteit (2 vormen, nader duiden), besmet adres, besmette postcode.

<sup>10</sup> IMS: identity management systeem; registratie in IMS is noodzakelijk voor toegang in FSV.

<sup>11</sup> En geregistreerd in (Agile)Feature F18.045, Aanpassingen FSV v.0.5, dd. 22-10-2018.



## B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

### 11. Rechtsgrond

**Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.**

**Algemene bepalingen AWR?**

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<sup>12</sup> 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 derden met een wettelijke taak: artikel 6 lid 1 onder c AVG. (de informatieverzoeken). Het volledige proces van de externe informatieverzoeken is behandeld in de GEB 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 dat is toegestaan.**

<sup>12</sup> 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.



1. **Informatieverzoeken** bevatten mogelijk **bijzondere**<sup>13</sup> 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**<sup>14</sup> (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**<sup>15</sup> (**fraude**) signalen kunnen **bijzondere** persoonsgegevens bevatten. De 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<sup>16</sup> 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.**

---

<sup>13</sup> Direct of indirect. Bv. in de context van zorgtoeslag kan een gegeven indirect iets over de gezondheidstoestand van een betrokkene zeggen.

<sup>14</sup> 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.

<sup>15</sup> Zoals MMA, Track/Justis, FIU, ISZW e.d.

<sup>16</sup> „verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unirechtelijke of lidstaatrechtelijke bepalingen die voldoende waarborgen ... bieden.“ Zorgtoeslag van Toeslagen is een tegemoetkoming in de kosten voor een zorgverzekering, die inkomensafhankelijk is.



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 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<sup>17</sup>) 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/renseignements vanuit het (ten dele statistisch onderbouwde) ervaringsgegeven<sup>18</sup> 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 gegevens 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.

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 selectie criterium geldt, wordt geen rekening gehouden met de context en hiervan afgeleid met mogelijk (ontrechte) 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, rolfhankelijk) 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, rolfhankelijk) zonder een goed ingerichte need-to-know-structuur en het ontbreken van logging en monitoring vormt daarbinnen een risico.

## 14. Noodzaak en evenredigheid

**Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.**

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

<sup>17</sup> 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.

<sup>18</sup> Bron: DF&A



**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 betrokkene

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

Het karakter van de verwerkingsgrondslagen voor opname van (persoons)gegevens 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 gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

### 16. Risico's

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

- a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
  - b. de oorsprong van deze gevolgen;
  - c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
  - d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.
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'.
  2. **Onvoldoende onderscheid tussen een informatieverzoek en een signaal maar ook betekenis/gewicht van de informatie, leidt tot mogelijke stigmatisering van betrokkene ('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/of 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.

- 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/schoningsfunctionaliteit worden verwerkt en het ontbreken van massale-archiverings-/schoningsfunctionaliteit. Dit heeft tot gevolg dat er een incompleet, onjuist en/of gedateerd beeld van betrokkene ontstaat in de (verdere) verwerking van gegevens, ook buiten FSV, zoals de risicopostselectie (bv. bij DF&A) en toetsing in FSV in geval van individuele klantbehandeling. Dit kan aanzienlijke 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<sup>19</sup> 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'<sup>20</sup> 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

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

<sup>19</sup> Waarvan ongeveer 10% (509) inactief, dd dec 2018.

<sup>20</sup> Fenomeen dat ontstaat als personen zich anders gaan gedragen vanwege een mogelijke privacy-impact. Doorgaans betrokkene (belastingplichtigen), in dit geval medewerkers.

## 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.**

Als hoofdmaatregel wordt een herontwerp / migratie van FSV naar een nieuwe opzet<sup>21</sup> geadviseerd. Daarmee kunnen, met als uitgangspunt privacy by design en default, de designeerde risico's worden weggenomen. Borg dat de migratie wordt gedaan in combinatie met processuele maatregelen als procesuniformering<sup>22</sup>, work-flow-management, zicht en zeggenschap op en over de verdere verwerking van data buiten FSV en voldoende controle daarop.

Herontwerpaspecten gerelateerd aan privacy-risico's zijn dan: gegevenskwaliteit (metadatering van de betekenis / waarde van gegevens waaronder het 'gewicht' van een signaal en het onderscheid tussen een signaal en een informatieverzoek), ontwikkelen van systeemfunctionaliteit en vastleggen van meta-data met betrekking tot de bewaar/archiveringstermijn, organiseren en reguleren van (al dan niet geautomatiseerde<sup>23</sup>) datadistributie, need-to-know toegang tot data, logging- en monitoring van gebruik.

Mede afhankelijk van het tijdpad van de voorgestelde migratie/herontwerp, moet een aantal voorlopige maatregelen in de huidige opzet van FSV worden genomen, in het bijzonder ten aanzien van:

1. Het toetsen van de bestaande autorisaties (en mogelijk het aantal rollen) op noodzakelijkheid en actualiteit/geldigheid gevolgd door 'schoning' op basis van de uitkomst van de toetsing.
2. Het schonen van een aantal jaarlagen (bv jongste signaal over betrokkene is > x jaar).
3. a. Het aanbrengen van onderscheid tussen een signaal en een informatieverzoek bij verdere verwerking van FSV data in andere informatiesystemen / analyseomgevingen.  
b. (indien mogelijk) het zo objectief mogelijk vastleggen van het 'gewicht' van een signaal.  
c. Implementeren van een uniforme werkwijze (bv. Conform/analoog proces Toeslagen) om op fiscale relevantie onderzochte informatieverzoeken op te voeren als signaal en deze signalen (verder) te verwerken in plaats van de informatieverzoeken.
4. Het verwijderen/de-activeren (of nader beperken qua gebruikersgroep) van massale en/of integrale exportfunctie(s).
5. 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 en eerder vastgelegde oplossingsmogelijkheden voor herbouw.

<sup>21</sup> 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 fraudecoördinator).

<sup>22</sup> 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.

<sup>23</sup> Denk aan opslag in en distributie vanuit datafundamenten ipv handmatig overzetten naar (S+)systemen zoals nu gebeurt.







Maatregelen nemen

Privacybewustwording

Doelbinding

PIA

Noodzaak

Effecten in kaart

Bescherming van  
persoonsgegevens

Risico's minimaliseren

Richtinggevend

Rechtsgrond

Met open vizier

by lage 0



Ministerie van Financiën

DEPARTEMENTAAL VERTROUWELIJK

Handleiding Gegevensbeschermingseffectbeoordeling (GEB/DPIA) Belastingdienst

Versie 00

Datum 14 mei 2019  
Status Concept

CONCEPT



## Colofon

**Titel** Handleiding Gegevensbeschermingseffectbeoordeling  
(GEB/DPIA) Belastingdienst

**Auteur(s)** Persoonsgegevens

---

## Bijlagen

**Inlichtingen** **IV&D**  
Privacy Officer

Persoonsgegevens

## Versiebeheer

Versie	Status	Datum	Gedeeld intern	Vastgesteld
00	Concept (intern)	4 juli 2019	Met Datacoördinatoren	-

## Inhoud

### Inhoudsopgave

#### Inleiding

- 1.1 Wat is een GEB/DIPA?
  - 1.2 In welke gevallen dient een DPIA te worden uitgevoerd?
  - 1.3 Wie voert een GEB/DPIA uit?
  - 1.4 Hoe verhoudt de GEB/DPIA zich tot andere Instrumenten?
  - 1.5 Processtappen GEB/DPIA
  - 1.6 Waar kan ik meer informatie vinden?
-

## Inleiding

De Belastingdienst vindt het belangrijk om de gegevensbescherming te verbeteren. Om de (Europese) wet- en regelgeving na te leven is er een GEB/DPIA als instrument. De AVG en de Wet politiegegevens<sup>1</sup> (Wpg) schrijven voor dat een gegevensbeschermingseffectbeoordeling (GEB/DPIA)<sup>2</sup> wordt uitgevoerd bij bepaalde verwerkingen van persoonsgegevens. Ook bij de Belastingdienst moeten voor bepaalde gegevensverwerkingen GEB/DPIA's worden uitgevoerd.

Dit document beschrijft de procedure die de Belastingdienst hanteert voor de uitvoering van een GEB/DPIA volgens het 'Model gegevensbeschermingseffectbeoordeling rijkdienst'. Deze procedurebeschrijving is een aanvulling op procedure van het kerndepartement, maar dan toegespitst op de Belastingdienst.

### 1.1 Wat is een GEB/DPIA?

Door het uitvoeren van een PIA wordt de bescherming van persoonsgegevens op een gestructureerde manier onderdeel van de belangenafweging en besluitvorming van voorgenomen beleid, regelgeving en (ICT-)projecten binnen de rijkdienst. Dit verhoogt de kwaliteit van de besluitvorming.

Een GEB/DPIA is in de eerste plaats richtinggevend het is een instrument om de risico's voor betrokkenen bij het verwerken van persoonsgegevens in kaart te brengen en te beoordelen. Daarnaast is een GEB/DPIA corrigerend. Op basis van de geconstateerde risico's kunnen de eerder gemaakte keuzes worden heroverwogen door bijvoorbeeld voor een minder inbreukmakende oplossing te kiezen. Er worden ook (aanvullende) maatregelen getroffen om de risico's te verkleinen of, indien mogelijk, weg te nemen.

#### Maatregelen

Het is van belang dat de set aan maatregelen voortvloeiend uit de GEB/DPIA in het betreffende proces wordt geïmplementeerd en gehandhaafd. De maatregelen kunnen zowel organisatorisch als technisch van aard zijn. Hier wordt duidelijk dat het juridische- en het technische (o.a. informatiebeveiliging) samen vallen.

Het is van belang dat de verwerkingen van persoonsgegevens blijvend voldoen aan de eisen die de Avg stelt. Zowel in het VIR 2007 als in de AVG en de Wpg wordt gesteld dat de verantwoordelijke een planning- en controlcyclus (plan-do-check/learn-act cyclus) heeft ingericht om te borgen dat de beveiliging en de verwerking van persoonsgegevens steeds adequaat zijn voor de huidige stand van de techniek en de organisatie.

<sup>1</sup> EU-Richtlijn gegevensbescherming bij opsporing en vervolging.

<sup>2</sup> De AVG spreekt van een Gegevensbeschermingseffectbeoordeling (GEB). Engelse vertaling: Data Protection Impact Assessment (DPIA).

#### Model GEB/DPIA

Voor het uitvoeren van een GEB/DPIA is een standaard model beschikbaar.<sup>3</sup> Het 'Model gegevensbeschermingseffectbeoordeling rijksdienst' wordt hiervoor gebruikt. Het Rijksmodel biedt ruimte om de verwerking van persoonsgegevens in elke stap van het betreffende proces uitgebreid te beschrijven. Door het proces te beschrijven ontstaat een correct beeld met betrekking tot de risico's van de daadwerkelijke verzameling en verwerking van persoonsgegevens.

Het Rijksmodel is voorzien van een handreiking en van een korte toelichting bij iedere vraag. De GEB/DPIA is pas volledig wanneer het voorblad, de management samenvatting en alle 17 punten uit het Rijksmodel zijn voorzien van een antwoord en de overweging daartoe.

Met opmerkingen op de verwerking, opsteller, versiebeheer, management samenvatting, het uitgewerkte model met de antwoorden op de vragen en de benodigde bijlagen.

Vragen om het model aan te passen en te plaatsen op de BD site. De link hiervan in dit document opnemen.

### 1.2 In welke gevallen dient een GEB/DPIA te worden uitgevoerd?

Een GEB/DPIA moet in de volgende gevallen **verplicht** worden uitgevoerd:

1. bij de ontwikkeling van beleid en regelgeving die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien;
2. bij voorgenomen verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.

In de tweede situatie is een GEB/DPIA dus niet in alle gevallen verplicht voor voorgenomen overheidsverwerkingen, maar alleen bij verwerkingen met een hoog risico<sup>4</sup>. Daarvoor is de AVG leidend.

Een GEB/DPIA van voorgenomen overheidsverwerkingen is in ieder geval **vereist** in de volgende gevallen:

- a. een systematische en uitgebreide beoordeling van persoonlijke aspecten, die is gebaseerd op geautomatiseerde verwerking, en waarop besluiten worden gebaseerd waaraan rechtsgevolgen zijn verbonden of die de betrokkenen op vergelijkbare wijze wezenlijk treffen;
- b. grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten;
- c. stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten;
- d. wanneer de Autoriteit persoonsgegevens heeft geoordeeld dat een GEB/DPIA verplicht is.

<sup>3</sup> [Link naar model](#) (komt nog)

<sup>4</sup> Zie hiervoor het Model gegevensbeschermingseffectbeoordeling rijksdienst, pag. 7.



### 1.3 Hoe verhoudt een GEB/DPIA zich tot andere instrumenten?

Een GEB/DPIA wordt naast, zo nodig in afstemming met andere hulpmiddelen voor ontwikkeling van regelgeving en overheidsverwerkingen ingezet; denk aan de uitvoeringstoets.<sup>5</sup>

Andere instrumenten voor het beoordelen van risico's op het gebied van gegevensbescherming kunnen een verplichte GEB/DPIA **niet** vervangen.<sup>6</sup>

### 1.4 Wie voert een GEB/DPIA uit?

Proces GEB/DPIA op hoofdlijnen

- A. Concerndirectie IV&D stelt de kaders voor informatiebeveiliging en privacy voor de Belastingdienst en biedt waar nodig inhoudelijke ondersteuning.
- B. De directeur die verantwoordelijk is voor het proces en/of informatiesysteem heeft de rol van (gemandateerde) Verwerkingsverantwoordelijke.
- C. Namens de Verwerkingsverantwoordelijke begeleidt de contactpersoon voor de gegevensbescherming, de zogenoemde Data Coordinator (DC) de uitvoering van de GEB/DPIA.
- D. De GEB/DPIA wordt uitgevoerd door een multidisciplinair team. Deze bestaat uit een inhoudelijk deskundige, een informatiebeveiliging, een deskundige op het gebied van gegevensbescherming, een IT'er en de coördinator en/of penvoerder.
- E. Toetsing aan de hand van het privacy-beleid van de Belastingdienst vindt plaats door de PO.
- F. Toetsing aan de hand van het informatiebeveiligingsbeleid vindt plaats door de Chief Information Security Officer (CISO). Bij de Belastingdienst staat in het HBB beschreven op welke wijze de standaard risico's (departementaal vertrouwelijk) moeten worden afgedekt. Een GEB/DPIA kan ervoor zorgen dat er aanvullende maatregelen moeten worden getroffen.
- G. Intern toezicht op de GEB/DPIA-procedure en het Concept GEB/DPIA-verslag vindt plaats door de Functionaris Gegevensbescherming (FG).
- H. CIO beoordeelt aan de hand van de adviezen of de voorgenoemde maatregelen afdoende zijn ondervangen. En geeft een oordeel over de restrisico's.
- I. De GEB/DPIA wordt retour gestuurd aan de directeur, door tussenkomst van de DC. De directeur stelt de GEB/DPIA vast met inachtneming van alle adviezen.
- J. De registratie in het Verwerkingsregister vindt plaats door de uitvoerende DC. De vastgestelde GEB/DPIA en overige relevante documenten worden aan de registratie toegevoegd.
- K. Borging van de kwaliteit van het register geschiedt in het kader van het reguliere beheer (planning en control cyclus) door de PO en CISO.

<sup>5</sup> Zie voor de hulpmiddelen voor ontwikkeling van regelgeving en overheidsverwerkingen het Model gegevensbeschermingseffectbeoordeling rjksdienst, pag. 8.

<sup>6</sup> Binnen de Belastingdienst wordt met verschillende andere instrumenten gewerkt zoals een WMK-toets, checklist of quikscan.

### 1.5 Processtappen GEB/DPIA

<b>Stap 1</b>	
<b>Wijziging van het proces</b>	
<b>Input</b>	Iedere voorgenomen nieuwe verwerking of wijziging van een bestaande verwerking dient gepaard te gaan met een analyse op het betreffende proces. Op deze wijze kan tijdig worden vastgesteld of er al dan geen privacy gerelateerde gegevensverwerkingen plaatsvinden welke specifieke borging vereisen volgens de AVG.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De directeur signaleert de (voorgenomen) wijziging/introductie van een informatiedienst en/of bron en informeert de domeinarchitect, een MT-lid en de DC.</li> <li>2. De directeur geeft de DC opdracht tot initiatie van de GEB/DPIA procedure.</li> <li>3. De directeur stelt IV&amp;D op de hoogte met betrekking tot het voornemen een GEB/DPIA te starten.</li> </ol>
<b>Output</b>	De DC neemt de opdracht aan en gaat over tot het doen van een Quikscan. <sup>7</sup> Bij vragen met betrekking tot het uitvoeren van een GEB/DPIA of een Quikscan kan de DC ondersteuning vragen van de PO.  (Quikscan: Voor het uitvoeren van een Quikscan dienen de vragen onder 1.2 (wanneer is een GEB/DPIA verplicht) beantwoord te worden.)
<b>Opmerkingen</b>	Een GEB/DPIA is een momentopname; het kan zijn dat de omstandigheden veranderen. Het is dan ook van belang om een GEB/DPIA periodiek te herhalen.

<b>Stap 2</b>	
<b>Wel of geen GEB/DPIA?</b>	
<b>Input</b>	Opdracht van de verantwoordelijke aan de DC.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De DC toetst of er al dan niet een GEB/DPIA dient te worden uitgevoerd.</li> <li>2. Wanneer er <b>geen</b> GEB/DPIA noodzakelijk is, moeten er in het kader van informatiebeveiliging alsnog risico's in kaart worden gebracht voor die specifieke verwerking. Als er geen specifieke risico's aanwezig zijn, kan worden volstaan met het toepassen van de maatregelen uit de Baseline Informatiebeveiliging Rijksdienst 2017, basis beveiligingsniveau 2.</li> </ol>
<b>Output</b>	Er zijn twee uitkomsten mogelijk: er dient <u>wel</u> of <u>geen</u> GEB/DPIA te worden uitgevoerd.  <b>Wel:</b> - De DC gaat over tot het uitvoeren van de GEB/DPIA.

<sup>7</sup> Quikscan: artikel 35 Avg en artikel 27, 28 van de Richtlijn.

	<p>Geen:</p> <ul style="list-style-type: none"> <li>- De DC legt de uitkomst van de Quikscan voor aan de directeur;</li> <li>- De uitkomst van de Quikscan wordt door de directeur formeel bekrachtigd;</li> <li>- De formele uitkomst van de Quikscan wordt door de DC in het verwerkingsregister geregistreerd;</li> <li>- De DC informeert de PO over de registratie;</li> <li>- De registratie in het verwerkingsregister wordt door de PO en de FG op kwaliteit gecontroleerd.</li> </ul>
<b>Opmerkingen</b>	-

<b>Stap 3</b>	
<b>Uitvoeren GEB/DPIA</b>	
<b>Input</b>	Indien er uit de uitkomst van de Quikscan volgt dat een GEB/DPIA noodzakelijk is, gaat de DC over tot het begeleiden daarvan.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De DC organiseert een of meerdere groepssessies waaraan tenminste de ketenmanager, de informatiebeveiliging, de domeinarchitect, de inhoudelijk medewerker en het MT-lid betrokken worden voor de uitvoering van de GEB/DPIA;</li> <li>2. De DC voert de GEB/DPIA uit aan de hand van het Rijksmodel;</li> <li>3. De DC stelt de eerste conceptversie van de GEB/DPIA-rapportage op en biedt deze aan de directeur aan.</li> </ol>
<b>Output</b>	Eerste concept versie rapportage GEB/DPIA.
<b>Opmerkingen</b>	-

<b>Stap 4</b>	
<b>Accordering eerste concept rapportage GEB/DPIA</b>	
<b>Input</b>	Eerste concept rapportage GEB/DPIA.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De directeur bekrachtigt de eerste conceptversie van de GEB/DPIA-rapportage (de directeur gaat akkoord met de beschrijving van de verwerking nog niet met de GEB/DPIA);</li> <li>2. De directeur biedt de eerste conceptversie van de GEB/DPIA-rapportage aan PO aan.</li> </ol>
<b>Output</b>	Eerste conceptversie PIA rapportage
<b>Opmerkingen</b>	-

<b>Stap 5</b>	
<b>Toetsing Kwaliteitskaders (BIR 2017 en Privacy)</b>	
<b>Input</b>	Eerste conceptversie rapportage GEB/DPIA.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De PO toetst de eerste conceptversie van de GEB/DPIA-rapportage aan de kaders van de meest recente versie van de privacybeleidskaders;</li> </ol>

Met opmerkingen ingevuld wordt BIO

	<ol style="list-style-type: none"> <li>2. De CISO toetst de GEB/DPIA-rapportage aan de meest recente versie van de Baseline Informatiebeveiliging Rijksdienst (BIR);</li> <li>3. De DC verwerkt het resultaat van de toets tot een aangepast concept van de GEB/DPIA-rapportage;</li> <li>4. De PO biedt het aangepaste concept GEB/DPIA-rapportage aan de FG aan.</li> </ol>
<b>Output</b>	Aangepast concept versie rapportage GEB/DPIA.
<b>Opmerkingen</b>	-

<b>Stap 6</b>	<b>Toetsing tweede concept rapportage GEB/DPIA</b>
<b>Input</b>	Tweede conceptversie rapportage GEB/DPIA.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De FG toetst het aangepaste concept van de GEB/DPIA-rapportage aan de meest recente kaders van de AVG en anderszins relevante privacywetten en regelgeving.</li> <li>2. De DC ontvangt het aangepaste concept van de PO en verwerkt het resultaat in de GEB/DPIA-rapportage;</li> <li>3. De PO biedt het aangepaste concept GEB/DPIA-rapportage aan de CIO aan, waarna de CIO toetst of alle risico's zijn onderkend, of er sprake is van restrisico's en of de voorgenomen maatregelen afdoende zijn;</li> <li>4. CIO stuurt het aangepaste concept naar de PO.</li> <li>5. De DC ontvangt het aangepaste concept van de PO. De DC stuurt vervolgens het aangepaste concept GEB/DPIA-rapportage naar de directeur.</li> </ol>
<b>Output</b>	Aangepaste concept versie GEB/DPIA-rapportage.
<b>Opmerkingen</b>	-

<b>Stap 7</b>	<b>Vaststelling GEB/DPIA-rapportage</b>
<b>Input</b>	Aangepaste conceptversie GEB/DPIA-rapportage.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De directeur bekrachtigd het aangepaste concept van de GEB/DPIA-rapportage;</li> <li>2. De directeur draagt de formeel vastgestelde GEB/DPIA over aan de DC</li> </ol>
<b>Output</b>	Vastgestelde GEB/DPIA-rapportage.
<b>Opmerkingen</b>	-

<b>Stap 8</b>	<b>Registratie in Verwerkingsregister</b>
<b>Input</b>	Vastgestelde GEB/DPIA-rapportage.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De directeur geeft de DC de opdracht de formeel vastgestelde GEB/DPIA op te nemen in het verwerkingsregister (als bijlage bij de verwerking);</li> <li>2. De DC draagt zorg voor het opnemen van alle relevante documenten in het verwerkingsregister (denk bijvoorbeeld aan de GEB/DPIA en verwerkersovereenkomst.)</li> </ol>



<b>Output</b>	Vastgestelde GEB/DPIA-rapportage en eventuele andere relevante documenten worden opgenomen in het verwerkingsregister.
<b>Opmerkingen</b>	-

<b>Stap 9</b>	<b>Kwaliteitscontrole verwerkingsregister</b>
<b>Input</b>	Vastgestelde GEB/DPIA-rapportage opgenomen in het verwerkingsregister.
<b>Activiteiten</b>	1. De PO toetst de registratie van de DC in het verwerkingsregister. Indien noodzakelijk past de DC de registratie aan;
<b>Output</b>	Vastgestelde GEB/DPIA-rapportage en eventuele andere relevante documenten worden opgenomen in het verwerkingsregister.
<b>Opmerkingen</b>	-

<b>Stap 10</b>	<b>Gevolg geven aan de maatregelen voortvloeiend uit de GEB/DPIA</b>
<b>Input</b>	GEB/DPIA-rapportage.
<b>Activiteiten</b>	<ol style="list-style-type: none"> <li>1. De directeur geeft opdracht aan de medewerkers van het betreffende proces (zoals de inhoudelijke medewerker, CISO, domeinarchitecten etc.) de maatregelen die voortvloeien uit de GEB/DPIA te implementeren.</li> <li>2. De directeur en de medewerkers hanteren hierbij de planning- en controlcyclus.</li> <li>3. De medewerkers stellen periodiek een rapportage op met betrekking tot de voortgang van de implementatie.</li> <li>4. De rapportage wordt verstuurd aan de PO en de directeur.</li> <li>5. Aan de hand van de rapportage kan de PO waar nodig bijsturen.</li> </ol>
<b>Output</b>	Een proces dat in het kader van privacy en informatiebeveiliging naar de stand van de techniek en de organisatie adequaat is.
<b>Opmerkingen</b>	Het doel van de GEB/DPIA is het inventariseren van risico's die door de verwerking van persoonsgegevens ontstaan. Naar aanleiding van de GEB/DPIA wordt er een set aan organisatorische- en technische maatregelen geformuleerd. Deze set aan maatregelen dient vervolgens geïmplementeerd te worden in het betreffende proces. De planning- en controlcyclus zorgt ervoor dat er continue aandacht is voor wijzigingen in het proces en de bijbehorende risico's.

<b>Stap 11</b>	<b>Herijken GEB/PIA</b>
<b>Input</b>	GEB/DPIA-rapportage.

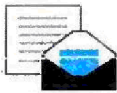
Activiteiten	
	<ol style="list-style-type: none"><li data-bbox="521 566 1045 633">1. De directeur geeft de opdracht aan de DC van het betreffende proces om bij een voorgenomen wijziging van het proces en/of de risico's een GEB/PIA uit te laten voeren.</li><li data-bbox="521 633 1045 701">2. De directeur geeft opdracht aan de DC van het betreffende proces de GEB/DPIA, in ieder geval, eens in de drie jaar de DPIA opnieuw uit te laten voeren.</li><li data-bbox="521 701 1045 754">3. Zie stap 1 van deze handleiding en volg de cyclus zoals beschreven.</li></ol>

### 1.6 Waar kan ik meer informatie vinden?

Voor meer informatie over het uitvoeren van een GEB/DPIA kun je terecht op de website van de Autoriteit Persoonsgegevens.<sup>5</sup>

<sup>5</sup> <https://autoriteitpersoonsgegevens.nl/>





**Fw: Betr: Fw: Restant vragen AP inzake FSV**

Persoonsgegevens

14-07-2020 10:59

Overzicht: Dit bericht is beantwoord.

deel 2. Laat maar weten of dit voldoende is

----- Doorgestuurd door Persoonsgegevens op 14-07-2020 10:59 -----

Van: Persoonsgegevens  
 Aan: Persoonsgegevens @Belastingdienst  
 Cc: Persoonsgegevens @Belastingdienst, Persoonsgegevens @Belastingdienst  
 Datum: 14-07-2020 08:50  
 Onderwerp: Betr: Fw: Restant vragen AP inzake FSV

Hier Persoonsgegevens

helpt dit?

Begin doorgestuurd bericht:

**Van:** Persoonsgegevens @belastingdienst.nl>  
**Datum:** 27 februari 2020 om 21:04:00 CET  
**Aan:** Persoonsgegevens @belastingdienst.nl>  
**Kopie:** Persoonsgegevens @belastingdienst.nl>  
 Persoonsgegevens @belastingdienst.nl>  
**Onderwerp:** FSV is uit de lucht

Persoonsgegevens

Ik heb de load balancer er tussen uit gehaald, waardoor de site van FSV niet meer bereikbaar is.

← → ↻ 🏠 🔒 anna.belastingdienst.nl/#/logging

📱 Apps 🌐 Intranet ★ Bookmarkmanager 📁 Geïmporteerd TN CRUD Operations i... 🌱 Bootstrap Coll

ANNA LOGGING	
TIMESTAMP	DESCRIPTION
2020-02-27 20:57:48	Delete an existing virtual ip
2020-02-27 20:37:44	Create a new endpoint



## Delete an existing virtual ip

**TIMESTAMP** 2020-02-27T19:57:48Z

**INITIATED FROM**  at 10.96.70.149

### RESULT

**LOAD BALANCER NAME**

**PROFILE LABEL** Default HTTPS with HTTP redirect

### TARGETS

**NETWORK ADDRESS** 10.224.24.77

**TRACE ID**

No matches? Check your search window



Vriendelijke groet

**MCC - Center DotNet**

**Generieke Business Services (GBS)**

**Belastingdienst**

John F. Kennedylaan 8 | 7314 PS | Apeldoorn |

Met vriendelijke groeten,

**Generieke Business Services (GBS) - IV regulier**  
**Standaard Transactie Services (STS) O&M en MP**  
**IV Organisatie**

**Belastingdienst Walterboscomplex**

John F Kennedylaan 8 | 7314 PS | Apeldoorn | Gebouw G1 Flex  
Postbus 9050 | 7300 GM | Apeldoorn

Persoonsgegevens

[www.belastingdienst.nl](http://www.belastingdienst.nl)

woensdag afwezig

Persoonsgegevens

Hallo Persoonsgegevens Zie onderstaande vraag van Persoonsgegevens 13-07-2020 20:30:56

Van: Persoonsgegevens  
Aan: Persoonsgegevens @Belastingdienst, Persoonsgegevens @Belastingdienst  
Cc: Persoonsgegevens @Belastingdienst  
Datum: 13-07-2020 20:30  
Onderwerp: Fw: Restant vragen AP inzake FSV

Hallo Persoonsgegevens

Zie onderstaande vraag van Persoonsgegevens

Is het mogelijk om screenshots te maken van de log of configuratie dat aan kan tonen dat FSV offline gehaald is 27 februari ?  
Laat me even weten

Met vriendelijke groet,



Belastingdienst

Persoonsgegevens

**Belastingdienst / GBS & STS**

Laan van Westenenk 492 | 7334 DS | Apeldoorn | Quintax Noord | 1e etage  
Postbus 9050 | 7300 GM | Apeldoorn

----- Doorgestuurd door Persoonsgegevens op 13-07-2020 20:28 -----

Van: Persoonsgegevens  
Aan: Persoonsgegevens @Belastingdienst  
Cc: Persoonsgegevens@minfin.nl  
Datum: 13-07-2020 08:00  
Onderwerp: Restant vragen AP inzake FSV

Goedemorgen Persoonsgegevens

FSV is achter de rug (voor nu).  
Nu nog even restjes bezoek AP afhechten en ik kan mij weer focussen op "regulier" werk ;-)

Voor één restpunt heb ik jouw hulp nodig:  
De AP wil graag bewijs van het daadwerkelijk uitschakelen van FSV op 27 februari. Het mailtje van

Persoonsgegevens is reeds in het bezit van de AP, maar ze zien graag aanvullend (technisch) bewijs.

Kan jij op basis van logging oid laten achterhalen of er meer bewijs is van de acties die IV heeft uitgevoerd op de avond van de 27e februari?  
Hoor graag van je.

*Met vriendelijke groet,*

Persoonsgegevens

*Concerndirectie IV&Databeheersing  
Directoraat Generaal Belastingdienst  
Ministerie van Financiën*

Persoonsgegevens



