

Re: GRAAG SPOED - GRAAG ADVIES - FW: Advies inzake FSV [REDACTED] aan [REDACTED]
27.02.2020 20:56

Dag

Vanavond is het besluit genomen om fry uit te zetten.

Da heeft een geb./Pia opgesteld / laten stellen, deze was bij tv&d niet bekend?!, staar te dafelsk de maal door die ik verstuurd heb.

Girl

On 27 feb. 2020 om 12:17 heeft

@belastingdienst.nl> het volgende geschreven:

Bente

Naar aanleiding van onderstaande mail lijkt het me goed om even te overleggen over eventuele vervolgaankomsten FSV. Ik zou zelf graag willen weten wat er tot nu toe gebruik hebben gemaakt van dit systeem. Ook lijkt het me goed FSV's afzonderlijke verwerking op te nemen in het AVO-verwerkingsregister, zodat hierover vooraf: ik hoor graag welke denken jij daarover hebt.

Met vriendelijke groet,

Relaxingriener
Bureau Directie Ondersteuning GO
Crescentlaan 14 3528 CA Utrecht

M.05 - [REDACTED]
[REDACTED] bslodtngdlenet.nl
<http://www.bslodtngdlenet.nl>

Woensdag afwezig

Downloaded from  27.03.2020 12:11

[illegible]

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 bijzonder strafrechtelijke persoonsgegevens. Het staat buiten twijfel dat het verwerken van zulke gevoelige gegevens alleen mag plaatsvinden als dat verantwoord is. Dat is naar ik begrip 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 beschreven 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 ~~verleving~~ 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 daarevoor het volgende gesteld:

[] en []
zijn als gemandateerd verwerkingsverantwoordelijken aangewezen voor de respectievelijke wettelijke taken."

- Op dit moment is voor mij onvoldoende duidelijk of 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 de af lijnmanager die het betreft aantoonbaar (via een Plan van Aanpak) opvolging worden gegeven aan de aanbevelingen/verbetervoorstellen uit de PIA.

- De betrokkenheid [] 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 7.3.m. te herstellen.

Groot,

☐

Van: (SEORUF) <@minfin.nl>

Verzonden: woensdag 26 februari 2020 10:26

Aan: (RVA) <@minfin.nl>

CC: (MT) <@minfin.nl>; @belastingdienst.nl

@belastingdienst.nl; @belastingdienst.nl

Onderwerp: GRAAG SPOED - GRAAG ADVIES - FW: Advies inzake FSV

Urgentie: Hoog

Hoi ☐

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,

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

I +31 (0)
 M +31 (0)

@minfin.nl

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

Verzonden: donderdag 20 februari 2020 21:31

Aan: (MT) <@minfin.nl>

CC: (IV&D) <@minfin.nl>;

<[redacted]@minfin.nl> (BEDRUF)
 [redacted]@minfin.nl> [redacted]@belastingdienst.nl

Onderwerp: Re: Advies inzake FSV

Hierin [redacted]

Voor de volledigheid:

De Pla heeft versienummer 1.2. Een concept zijn, maar heeft dan de schijn tegen als de Pla nog in concept is en in de Pla staat moet bevindingen, dan nog heeft nu een verwerking in de lucht die op zijn minst dubieus te noemen is. Het aanpassen van de Pla maakt de verwerking niet automatisch legitiem. Tenzij natuurlijk de huidige Pla de werkelijkheid gewild aandoet. Maar zelfs in dat geval zou ik mij als [redacted] zorgen maken over deze specifieke verwerking.

Ik vul mijn advies dan ook aan met de aanbeveling om raast het stoppen met de verwerking, de Pla 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]

[redacted]

Concordirectie IV & Databasehoofding
 Directoraat Generaal Delastingdienst
 Ministerie van Financiën

M.06 [redacted]
 [redacted]@minfin.nl

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

Allen

Net [redacted] even gesproken.

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

Tevens zal ik morgen de eigenaar van de directies, die FSV gebruiken, vragen om tevens te rapporteren op de maatregelen van toegang, gebruik excel en schone 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 aannemen na beoordeling

van de PIA door de [redacted] NB. Het is een registratiesysteem, waarna een reguliere controle volgt. Er is in de zin geen indicatie op basis van dit gebruik dat er sprake is van vervolgschade voor burgers.

[redacted]

Verzonden met BlackBerry Work
(www.blackberry.com)

[...]

Van: [redacted] (TVB/DH) <[redacted]@minfin.nl>
 Dinsdag, donderdag 20 feb. 2020 7:11 PM
 Aan: [redacted] (MFD) <[redacted]@minfin.nl>
 Kwie! [redacted] (Zn minfin) <[redacted]@minfin.nl>.
 [redacted] (BEDRUF) <[redacted]@minfin.nl>.
 [redacted] (Relatiedienst.nl) <[redacted]@relatiedienst.nl>
 Onderwerp: Advies inzake FSV

[redacted]

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 comfort van informatiebeveiliging, zie hieronder mail aan [redacted] heb ik getracht een antwoord op te krijgen van de betrokken [redacted] en [redacted]

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 schorring/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 Relatiedienst 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:

[] (dan wel []) 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;

[] opdracht te geven de dumps actief op te sporen en te vernietigen (en te documenteren waar deze dumps zijn aangetroffen);

[] 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 []

Hallo []

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 systeamdumps, 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 verweride elementen"10 en het felt dat er ook niet zonder meer objectief getoetste of toetsbare signalen worden geregistreerd, maken dat het kamiter van sommige verweridingsvormen 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. aienemende "systemen" / verdere verwerkingen (DFA), 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 informatie vraag wordt bij verdere verwerking ook niet of niet juist gevoelen. Niet ieder informatie verzoek is op voorhand een fiscaal signaal."

- PIA beschrijft dat exporteren niet gelogd wordt. Informatie van [] 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 IMG (dus op basis van een rol). Op pagina 18 wordt het restrictie 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 velen 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 betwist.
- 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 (om dat 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 informatiejhalonn"
- "recent memo aan de Stas inzake Fraudemeldpunt"
- Applicatie "Inzicht"

Gevolgen:

Onder de verantwoordelijkheid van [redacted] 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.

[redacted]
[redacted]
Coördinatie IV&Data-beheersing
Directoraat Generaal Belastingdienst
Ministerie van Financiën

MCS [redacted]
[redacted] [@minfin.nl](mailto:[redacted]@minfin.nl)

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, herwaarschrijven, 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.