



Concept
voor discussie

AVG-onderzoek naar oud EH&I-producten bij DF&A

CONCEPT Rapport - AVG-onderzoek naar oud EH&I-producten bij DF&A,
Belastingdienst

A2000021206 CRA

20 november 2020

Inhoudsopgave

1. Achtergrond, doel, scope en aanpak	4
2. Managementsamenvatting	7
3. Detailoverzicht	11
Appendices	35
A – Lijst van interviews	
B – Bestudeerde documentatie	



© 2020 KPMG Advisory N.V., ingeschreven bij het handelsregister in Nederland onder nummer 33263682, is lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Cooperative ("KPMG International"), een Zwitserse entiteit. Alle rechten voorbehouden. De naam KPMG en het logo zijn geregistreerde merken van KPMG International.



1. Achtergrond, doel, scope en aanpak



1. Achtergrond, doel, scope en aanpak

Aanleiding

Om de taken van de Belastingdienst sneller en gericht uit te voeren, combineert DF&A (persoonsgegevens uit verschillende systemen om deze vervolgens op te werken tot datafundamenten. Het werken met (persoons)gegevens hangt daarbij nauw samen met de bescherming van privacy. Burgers moeten erop kunnen vertrouwen dat er binnen de systemen van DF&A op een rechtmatige, zorgvuldige en transparante manier met persoonsgegevens wordt omgegaan.

Doel

Binnen DF&A bestaat daarom de wens om een onderzoek te laten uit voeren naar de circa 50 oud-producten – waarvan 5 netwerken, 17 advies en 28 producten – van het voormalige EH&I welke zijn overgedragen aan het huidige DF&A. Doel is om te onderzoeken of deze EH&I-producten voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Archiefwet en uw Quality Assurance (QA) kaders, inclusief de door DF&A intern gehanteerde gouden regels en overige van toepassing zijnde wet- en regelgeving zoals het juridisch kader dat is gehanteerd in de rapportage 'Verwerking risico-selectiesignalen voor toezicht' d.d. 10 juli 2020.

Scope en aanpak

Om binnen de beoogde tijdlijnen gedegen antwoord te kunnen geven op de onderzoeksvraag, hanteren wij een gefaseerde aanpak die ons in staat stelt binnen de beoogde tijdlijnen tot de kern te komen van uw onderzoeksvraag. Een uitgebreide beschrijving van onze gelaagde aanpak volgt in het vorige hoofdstuk, 'Ons plan van aanpak'. Met betrekking tot de scope, betekent dit het volgende:

- Wij zullen ons met betrekking tot de door u gemaakte selectie van de 50 EH&I-producten, alle 50 producten en diensten onderwerpen aan een gelijkwaardige mate van diepgang. EH&I-producten die echter een laag privacy risicoprofiel vertonen, zullen minder uitvoerig worden gerapporteerd, nu de meeste normen en standaarden niet van toepassing zijn.

Met een laag risicoprofiel doelen wij op EH&I-producten die geen persoonsgegevens blijken te verwerken, producten die enkel basisgegevens (aldus

NAW-gegevens of zakelijke contactgegevens) verwerken, producten die niet langer in gebruik zijn of uitgezet zijn en/of producten die enkel faciliterend zijn aan de gegevensverwerking en niet de bron zijn van de gegevensverwerking

- De EH&I-producten die een verhoogd privacy risicoprofiel vertonen, hebben wij onderworpen aan een globale analyse waarbij wij ons richten op de mate waarin deze producten voldoen aan de basisbeginselen van de AVG.
- Ons onderzoek omvat niet het uitvoeren van Gegevensbescherming effectbeoordelingen (GEB's) op EH&I-producten of het analyseren van het al dan niet correct door de Belastingdienst vaststellen van de wettelijke grondslag voor het desbetreffende EH&I-product (of andere wettelijke vereisten).
- Onze inventarisatie is gebaseerd op ter beschikking gestelde documentatie en gehouden interviews, wij hebben geen analyse van de verwerkingen en hiervoor gebruikte systemen zelf gedaan.

Met betrekking tot de producten die vallen in categorieën 2 en 3 is nog een aantal zaken voorafgaand van het lezen van dit rapport van belang:

- FIOD account. Dit product is een paraplu voor andere FIOD-producten, dus niet als zodanig meegenomen in deze rapportage.
- Poort IH is niet meegenomen in de beoordeling omdat dit product geen verbinding met DF&A heeft. Het betreft hier enkel een vanuit DF&A gedetacheerd persoon.
- Met betrekking tot producten/diensten ben behoeve van OB en MKB is uitgegaan van de beredenering dat gegevens over rechtspersonen ook mogelijk persoonsgegevens kunnen bevatten en/of deze gegevens gevoelig kunnen zijn op basis van de definitie in de Gouden Regels van DF&A. Daarom zijn gegevens over de rechtspersoon gelijkgetrokken met persoonsgegevens in dit rapport.





1. Achtergrond, doel, scope en aanpak

Definities

Zoals in de aanpak op de vorige pagina beschreven zijn de producten tijdens het onderzoek in drie verschillende categorieën ingedeeld. Hieronder is zijn de 3 categorieën gedefinieerd:

- | | |
|-------------|---|
| Categorie 1 | Er worden geen persoonsgegevens verwerkt en de overige vereisten vanuit wet- en regelgeving, alsmede de door de Belastingdienst gestelde kaders zijn niet van toepassing, ofwel het EH&I-product of -dienst wordt uitgezet, of niet meer gebruikt per 1 september 2020. |
| Categorie 2 | Er worden persoonsgegevens verwerkt en/of de overige vereisten vanuit wet- en regelgeving, alsmede de door de Belastingdienst gestelde kaders zijn van toepassing, maar de persoonsgegevens zijn dusdanig basaal en triviaal (aldus NAW-gegevens, zakelijke contactgegevens) dat deze verwerking geen verhoogd risico oplevert. |
| Categorie 3 | Er worden (veel) persoonsgegevens verwerkt en/of er is sprake de verwerking van (veel) gevoelige of bijzondere persoonsgegevens of waarbij sprake is van een hoog risico verwerkingsactiviteit, zoals profilering. |

Ten aanzien van de producten en/of diensten die in categorieën 2 en 3 vallen is in het detailoverzicht een omschrijving opgenomen, welke betrokkene en persoonsgegevens betrokken zijn en welke risico's er zijn geïdentificeerd. Daarnaast wordt ook aangegeven welke documenten beschikbaar zijn gesteld en geven wij een indicatie van het risiconiveau waartoe het product en/of dienst naar aanleiding van onze analyse behoort. Het risiconiveau is Hoog, Midden of Laag.

- Een Laag risico wil zeggen dat het inherente risico (de aard en de omvang van de verwerking van persoonsgegevens), samen met de genomen maatregelen een laag risico opleveren op con-compliance met wet- en regelgeving.
- Een Midden risico wil zeggen dat het inherente risico groter is, en/of de genomen maatregelen aanzienlijke gebreken kent.
- Een Hoog risico wil zeggen dat het inherente risico hoog is, en dat er een of meerdere maatregelen niet genomen zijn.

Leeswijzer

Hierna volgt eerst een managementsamenvatting met een overzicht van de mate waarop de producten voldoen aan een aantal door ons geselecteerde kernvereisten uit de AVG, de Archiefwet en uw Quality Assurance (QA) kaders, inclusief de door DF&A intern gehanteerde Gouden Regels. Hierbij hebben wij een indeling gemaakt in i) voldoet, ii) voldoet niet, of iii) voldoet gedeeltelijk.

Deze managementsamenvatting sluit af met een algemene beschrijving van de aanpak en de definities. In hoofdstuk 3 vindt u per categorie een detailoverzicht van onze bevindingen per product of dienst.





2. Management-samenvatting

2. Managementsamenvatting (1/3)



Aanleiding en onderzoeksvraag

Om de taken van de Belastingdienst sneller en gericht uit te voeren, combineert DF&A (persoonsgegevens uit verschillende systemen en bronnen om deze vervolgens op te werken tot datafundamenten. Dit brengt vanzelfsprekend het verwerken van persoonsgegevens met zich mee. Het is daarom van belang om de privacyrisico's die gepaard gaan met de producten van DF&A inzichtelijk te maken.

DF&A heeft KPMG Advisory N.V. (hierna: 'KPMG') gevraagd een onderzoek te verrichten naar een aantal oud EH&I-producten en deze te toetsen aan de Algemene Verordening Gegevensbescherming (AVG), de Archiefwet en uw Quality Assurance (QA) kaders, inclusief de door DF&A intern gehanteerde Gouden Regels en overige van toepassing zijnde wet- en regelgeving zoals het juridisch kader dat is gehanteerd in de rapportage 'Verwerking risicoselectiesignalen voor toezicht' d.d. 10 juli 2020. De aanpak is in detail beschreven in de offerte d.d. 1 oktober 2020 met uw referentie 'UC20-716'.

Algemene Observaties

Documentatie

Voor ieder proces of product dat wordt ontwikkeld wordt een procedure gevolgd waarbij een WMK-toets wordt uitgevoerd en mogelijk ook andere toetsingen, zoals een QC-toets, AVG-scan of GEB. ² Het betrekking tot de oud-producten van EH&I is gebleken dat de meerderheid van de te onderzoeken producten en/of diensten niet onderworpen zijn aan dergelijke analyses. Als gevolg konden voor deze rapportage slechts voor een beperkt aantal producten de documenten worden geanalyseerd.

Verantwoordelijkheid

Het is niet altijd bekend of geformaliseerd wie/welk onderdeel binnen de Belastingdienst de uiteindelijke eigenaar is van de gegevens. Een aantal producten en/of diensten is het verstrekken van informatie, vervaardigd door een query op een datafundament door DF&A, aan één van de andere dienstonderdelen. Het is niet altijd bekend hoe er vervolgens met de gegevens door het desbetreffende onderdeel wordt omgegaan. Het risico bestaat dat de vooraf vastgestelde eisen en voorwaarden niet consistent worden nageleefd of als dat wel gebeurt, dit niet aantoonbaar is.

Hoog Risicoverwerkingen

Op basis van de interviews en documentatieonderzoek hebben wij een aantal hoog risicovolle gegevensverwerkingen geïdentificeerd, die verband houden met de volgende producten en/of diensten:

1 Zeer vermogende personen

Het gaat om uiterst vertrouwelijke gegevens over vermogende personen en diens verwanten, waarbij hoge risico's zijn geïdentificeerd in relatie tot de gestelde privacy-waarborgen.

• Gruff

Het gaat om uiterst vertrouwelijke gegevens over personen en diens verwanten, waarbij meerdere risico's zijn geïdentificeerd in relatie tot de gestelde privacy-waarborgen.

• FIOD Berlijn Trailer, FIOD Centraal punt BTW-fraude, FIOD – AMLC en Team aanpak risicovolle netwerken

Deze producten hebben allemaal betrekking op het opsporen van de georganiseerde misdaad en brengen daardoor een inherent risico met zich mee door de hoge mate van vertrouwelijkheid die deze gegevens hebben. Tegelijkertijd is een aantal maatregelen en waarborgen nog niet ingericht.

Overzicht van opmerkingen bij 20201125 1330 KPMG rapport - RL.pdf

Pagina: 7

	Nummer: 1	Auteur:	Onderwerp: Markering	Datum: 24-11-2020 12:42:44 +01'00'
---	-----------	------------------------------	----------------------	------------------------------------

Graag beheersmaatregelen op dit punt specificeren - lees: concreet maken

	Nummer: 2	Auteur:	Onderwerp: Markering	Datum: 25-11-2020 15:04:46 +01'00'
---	-----------	------------------------------	----------------------	------------------------------------

Onderscheid tussen gebruikte en ongebruikte producten maken svp

2. Managementsamenvatting (2/3)

Concept
voor discussie

Hieronder treft u een overzicht aan van alle producten en diensten die vallen in categorieën 2 en 3 en in welke mate de producten en/of diensten voldoen aan de hieronder weergegeven vereisten. De producten/diensten in categorie 1 hebben wij niet op deze indicatoren kunnen evalueren, aangezien er geen persoonsgegevens verwerkt worden en de overige vereisten vanuit wet- en regelgeving, alsmede de door de Belastingdienst gestelde kaders, niet van toepassing zijn, ofwel het EH&I-product of -dienst is of wordt uitgezet, of niet meer gebruikt vanaf 1 september 2020.

Naam	Documentatie ²	Rechtmatige grondslag	Doelbinding	Proportionaliteit	Opslag van gegevens	Gegevensuitwisseling (intern en extern)	Dataretentie	Toegangsrechten
Schoonmaakbranche	-	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Schijnconstructies	-	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Uitzendbranche	-	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
OB telefoonverzuim	-	+	+	+/-	+	+	-	+
OB tweeverzuim/ Veelverzuim	-	+	+	+/-	+	+	-	+
Bijzondere normen	-	+	+	+/-	+	+	+	+
Branche-informatie	+	+	+	+	+	+	+	+
FIOD Bijzondere Taken	-	+/-	+/-	+/-	+	+	+/-	+
SIDN	-	+	+	+	+	+	-	+

Referentietabel

+	Voldoet toereikend
+/-	Voldoet gedeeltelijk (is niet gedocumenteerd)
-	Voldoet niet (en/of is niet aangetoond)



© 2020 KPMG Advisory N.V., ingeschreven bij het handelsregister in Nederland onder nummer 33263682, is lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Cooperative ("KPMG International"), een Zwitserse entiteit. Alle rechten voorbehouden. De naam KPMG en het logo zijn geregistreerde merken van KPMG International.

Pagina: 8

I	Nummer: 1	Auteur:	Onderwerp: Markering	Datum: 24-11-2020 12:43:54 +01'00'
	Koppeling met DFEX en of DAPM maken t.b.v. traceerbaarheid			
T	Nummer: 2	Auteur:	Onderwerp: Ingevoegde tekst	Datum: 24-11-2020 12:44:57 +01'00'
	Waar is naar gekeken? Zijn de DQR board stukken ook bekeken?			

2. Managementsamenvatting (2/3)



Vervolg van overzicht van alle producten en diensten in categorieën 2 en 3.

Naam	Documentatie ¹	Rechtmatige grondslag	Doelbinding	Proportionaliteit	Opslag van gegevens	Gegevensuitwisseling (intern en extern)	Dataretentie	Toegangsrechten
Marktplaatsverzoek	-	+	+	-	+	+	-	+
DAS tool	+	+/-	+/-	+/-	+/-	+	+/-	+/-
Zeer vermogende personen	-	-	+	-	+	+	+	-
Directoraat-Generaal Fiscale Zaken	-	+/-	+/-	+/-	+/-	+/-	+/-	+/-
Gruff Netwerk-analysetool	-	+	+	-	+	+	-	+/-
FIOD Berlijn trailer	-	+	+/-	+/-	+	+	-	+
FIOD Centraalpunt BTW-fraude	-	+	+/-	+/-	+	+	-	+
FIOD – AMLC	-	+	+/-	+/-	+	+	-	+
Team aanpak risicovolle netwerken	-	+/-	+	+	+	+	-	+
Signaalanalyse postbus								

Referentietabel	
+	Voldoet toereikend
+/-	Voldoet gedeeltelijk (is niet gedocumenteerd)
-	Voldoet niet (en/of is niet aangetoond)



	Nummer: 1	Auteur:	Onderwerp: Ingevoegde tekst	Datum: 24-11-2020 12:47:10 +01'00'
In welke van deze gevallen is sprake van gegevens verwerking / data uitlevering / advies? Hoe is dat onderscheid gemaakt				



3. Detailoverzicht Categorie 1*

*Er worden geen persoonsgegevens verwerkt en de overige vereisten vanuit wet- en regelgeving, alsmede de door de Belastingdienst gestelde kaders zijn niet van toepassing, ofwel het EH&I-product of -dienst wordt uitgezet, of niet meer gebruikt per 1 september 2020.

3. Detailoverzicht



Producten/diensten met risicocategorie 1

De hieronder genoemde EH&I-producten of -diensten zijn per 1 september 2020 niet (meer) in gebruik.

Naam	DFEX-nummer	Toelichting
☐ voor Fiscale Zaken	DFEX-177	Niet in gebruik per 1 september 2020
Verschillen ABS en FLG	Niet aanwezig	Niet in gebruik per 1 september 2020
Gebruikelijk loon digra	Niet aanwezig	Niet in gebruik per 1 september 2020
Balansschulden	DFEX-20	Niet in gebruik per 1 september 2020. Is dit jaar niet uitgeleverd en wordt pas gedaan als er opnieuw een WMK + goedkeuring is gedaan
OB/LH Monitoring & KI&S-module	Niet aanwezig	Niet in gebruik per 1 september 2020

3. Detailoverzicht



Producten/diensten met risicocategorie 1

In de hieronder genoemde EH&I-producten of -diensten worden geen persoonsgegevens verwerkt en de overige vereisten vanuit wet- en regelgeving, alsmede de door de Belastingdienst gestelde kaders zijn niet van toepassing.

Naam	DFEX-nummer	Toelichting
	Niet aanwezig	Dit betreft een rol. Als er nieuwe fraudefenomenen opduiken, wordt in deze rol kennis tussen afdelingen uitgewisseld. Dat gebeurt op fenomeen-niveau; hierbij worden geen persoonsgegevens verwerkt.
	Niet aanwezig	Dit betreft een rol. Binnen deze rol wordt in bepaalde omstandigheden opdracht aan anderen gegeven tot het onderzoeken van een fraudefenomeen, bijvoorbeeld zoals het geval was bij turboliquidatie. In de rol zelf worden geen gegevens verwerkt, maar de uitvoering van de rol kan wel leiden tot het doen verwerken van persoonsgegevens. Als dit het geval is, dan loopt dit tegenwoordig via het stramen van DF&A, zoals bijvoorbeeld gebeurde bij het proces onverklaarbare inkomen en uitgaven. Er zijn geen oude producten of diensten bekend op basis waarvan persoonsgegevens verwerkt worden.
Fraude EOS-teams	Niet aanwezig	De fraude EOS teams kunnen contact opnemen met DF&A. Als ze vragen om een product of levering, dan loopt dat via huidige proces van DF&A. Er zijn geen oude producten of diensten bekend op basis waarvan persoonsgegevens verwerkt worden.
Fraudeteams Particulieren	Niet aanwezig	De fraude teams kunnen contact opnemen met DF&A. Als ze vragen om een product of levering, dan loopt dat via huidige proces van DF&A. Er zijn geen oude producten of diensten bekend op basis waarvan persoonsgegevens verwerkt worden.
Fraude deskundigenoverleg (FDO)	Niet aanwezig	Dit betreft een ketenstructuur binnen de Belastingdienst, waarbij fraude en ontwikkelingen met alle partijen overlegd worden. Hier worden Belastingdienstbreed trends en fenomenen besproken; er worden in dit verband geen persoonsgegevens gedeeld. In deze ketenstructuur zijn er geen oude producten of diensten bekend op basis waarvan persoonsgegevens verwerkt worden.
Manifestgroepfraude	Niet aanwezig	Dit betreft een overheidsbreed orgaan. Dit is een netwerkorganisatie, waarin kennis gedeeld wordt, maar geen persoonsgegevens. In deze netwerkorganisatie zijn er geen oude producten of diensten bekend op basis waarvan persoonsgegevens verwerkt worden.
Werkgroep RUB (risicovolle uitbetalingen) CAP	Niet aanwezig	Dit betreft een kennisoverleg en platform. Het CAP heeft overleg met de huisbankier waar kennis mee gedeeld wordt, met als doel op zoek gaan waar men elkaar kan ondersteunen. Dit betreft trends, risico-scenario's en andere indicatoren, maar geen individuele gevallen en dus geen persoonsgegevens.
Werkgroep faillissementsfraude (Min. JenV)	Niet aanwezig	Dit betreft kennisdeling met het ministerie van Economische Zaken, en heeft als doel te overleggen hoe faillissementsfraude aangepakt kan worden. In deze werkgroep worden geen individuele gevallen behandeld en dus ook geen persoonsgegevens verwerkt.
Intranetportal/Service4u		Dit betreft de intranetsite die draait op de infrastructuur van de Belastingdienst.

Pagina: 12

 Nummer: 1	Auteur:	Onderwerp: Markering	Datum: 25-11-2020 15:07:12 +01'00'
---	------------------------------	----------------------	------------------------------------

 Nummer: 2	Auteur:	Onderwerp: Notitie	Datum: 25-11-2020 15:08:24 +01'00'
---	------------------------------	--------------------	------------------------------------

Dit lijstje bestaat primair uit netwerkactiviteiten en externe contacten. Dit zijn geen producten. Waar wordt dat onderscheid gemaakt?

3. Detailoverzicht



Producten/diensten met risicocategorie 1 Er worden geen persoonsgegevens verwerkt en de overige vereisten vanuit wet- en regelgeving, alsmede de door de Belastingdienst gestelde kaders zijn niet van toepassing, ofwel het EH&I-product of -dienst wordt uitgezet, of niet meer gebruikt.		
Naam	DFEX-nummer	Toelichting
FIOD centraal punt faillissementsfraude	Niet aanwezig	Dit is een uitwisseling van kennis en ervaring op het gebied van faillissement en vermoedelijke fraude van DF&A naar de FIOD. Hierbij wordt gekeken naar risicovolle netwerken die mogelijk leiden tot frauduleuze faillissementen. Doelstelling is het voorkomen en vroegtijdig stoppen hiervan. Er is hierbij geen sprake van gegevenslevering. Er wordt niet op individuele basis, maar op een hoger abstractieniveau gedeeld. Soms worden casussen besproken aan de hand van actualiteiten. Over het algemeen geldt echter de regel dat indien uit een overleg een opdracht tot levering voortvloeit, het gaat via een aparte opdrachtstroom via portfolio moet lopen.
FIOD strategische opsporingsinformatie	Niet aanwezig	Het betreft hier een samenwerking tussen DF&A en FIOD Strategische Opsporingsinformatie waarbij kennis gedeeld wordt op basis van fenomenen en trends, bijvoorbeeld het Taxirapport. Er wordt geen informatie uitgewisseld over individuele casussen en er worden dus geen persoonsgegevens verwerkt.
FIOD Acquisitie	Niet aanwezig	Het betreft hier een samenwerking tussen DF&A en FIOD Acquisitie waarin fenomenen, trends, en ontwikkelingen worden besproken. Er worden geen individuele casussen en dus geen persoonsgegevens verwerkt.
FIOD IFGC Trendwatching-rapport Radicaal Samenwerken	Niet aanwezig	Het betreft een externe samenwerkings- en kennisplatform gericht op veiligheid, gefundeerd door V&J. Hier worden nooit persoonsgegevens uitgewisseld.
Voorlichting en Training Notariaat (KNB; extern)	Niet aanwezig	Het betreft hier een kennisoverdracht van DF&A, in samenwerking met Bureau Financieel Toezicht naar het notariaat. Het doel is het preventief adviseren om het fraudebewustzijn te verhogen, zodat ze aan de voorkant fraude tegen kunnen gaan. Daarnaast is er ook twee keer per jaar een overleg over fenomenen en hoe hiermee om te gaan.
Werkgroep faillissementsfraude (Min van J&V)	Niet aanwezig	Dit betreft een publiek-private samenwerking, waarin DF&A het notariaat ondersteunt met advies en kennis. Het gaat om voorlichting; er worden geen persoonsgegevens uitgewisseld.
Werkgroep RUB (risicovolle uitbetalingen)	Niet aanwezig	Het betreft hier een kennisuitwisseling met een externe partner. Hierbij worden geen persoonsgegevens uitgewisseld. Maar intern kan het wel een signaal opleveren dat het nader bestudeerd moet worden.
Selfservice UCA	DFEX-173	Het betreft geaggregeerde data inzake voorlopige aanslagen. De Selfservice UCA is een dashboardtool die beschikbaar is gesteld aan de Unit Concern Administratie ('UCA') binnen de Belastingdienst. De tool bevat dashboards met data op geaggregeerd niveau en is bedoeld om informatie te leveren ten behoeve van het grootboek van de Belastingdienst. De data die ten grondslag ligt aan de geaggregeerde data is gebaseerd op (voorlopige) omzet, banktransacties en schulden van ondernemingen.



3. Detailoverzicht categorie 2*

*Er worden persoonsgegevens verwerkt en/of de overige vereisten vanuit wet- en regelgeving, alsmede de door de Belastingdienst gestelde kaders zijn van toepassing, maar de persoonsgegevens zijn dusdanig basaal en triviaal (aldus NAW-gegevens, zakelijke contactgegevens) dat deze verwerking geen verhoogd risico oplevert.

3. Detailoverzicht



*R = Risiconiveau

*Doc = Beschikbare documentatie

Schoonmaakbranche				
Schijnconstructie				
OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEïDENTIFICEERDE RISICO'S	Doc*	R*
Deze activiteit betreft een incidentele informatieaanvraag inzake 'risicovolle' bedrijven in de schoonmaakbranche. Dit betreft een extern verzoek. De data uitwisseling berust op een convenant met partners, zijnde (o.a.) ministeriële. De data wordt verstrekt aan externe instanties (partners) op verzoek. Deze verzoeken vinden incidenteel plaats. De informatie ziet op rechtspersonen. De uitlevering heeft sinds 1 september 2020 niet plaatsgevonden en zal niet plaatsvinden zonder WMK-toets. De data wordt vervaardigd door een query uit te oefenen op een datafundament, waarna deze wordt vormgegeven in een Excel-bestand. Bij uitwisseling van data vanuit DF&A/MKB naar de externe partner is het Excel-bestand beveiligd met een wachtwoord. <i>Aangezien de uitlevering nog niet heeft plaatsgevonden (en de wijze waarop dit plaatsvindt) hebben wij niet kunnen vaststellen of het product voldoet aan de vereisten zoals is opgenomen in het overzicht van uit de managementsamen-vatting en dus de AVG, de Archiefwet en uw OA-kaders, inclusief de door DF&A intern gehanteerde Gouden Regels.</i>	De informatie ziet op rechtspersonen in de schoonmaakbranche die voldoen aan een bepaald risicoprofiel. De gegevens die verwerkt worden zijn vertrouwelijk op basis van het document 'Gouden Regels voor omgang met vertrouwelijke informatie'.	<i>Uitlevering van data heeft voorsnog niet plaatsgevonden dit jaar. Er zijn daarom geen risico's gedefinieerd.</i>		L
*incl. LSI: Fenomenen, risicodetectie subject, Grensoverschrijdend werk. Deze activiteit betreft een incidentele informatieaanvraag inzake 'risicovolle' bedrijven. Dit betreft een extern verzoek. De data uitwisseling berust op een convenant met de partners, zijnde ministeriële. De data wordt verstrekt aan externe instanties (partners) op verzoek. Deze verzoeken vinden incidenteel plaats. De informatie ziet op rechtspersonen. De uitlevering heeft sinds 1 september 2020 niet plaatsgevonden en zal niet plaatsvinden zonder WMK-toets. <i>Aangezien de uitlevering nog niet heeft plaatsgevonden (en de wijze waarop dit plaatsvindt) hebben wij niet kunnen vaststellen of het product voldoet aan de vereisten zoals is opgenomen in het overzicht van uit de managementsamen-vatting en dus de AVG, de Archiefwet en uw OA-kaders / Gouden Regels.</i>	De informatie ziet op rechtspersonen die voldoen aan een bepaald risicoprofiel. De gegevens die verwerkt worden zijn vertrouwelijk op basis van het document 'Gouden Regels voor omgang met vertrouwelijke informatie'.	<i>Uitlevering van data heeft voorsnog niet plaatsgevonden dit jaar. Er zijn daarom geen risico's gedefinieerd.</i>		L

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

WIK

WIK

GEB

GEB/AVG-scan

concept

discussie

*R = Risiconiveau
*Doc = Beschikbare documentatie

Uitzendbranche				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEïDENTIFICEERDE RISICO'S	Doc* R*
Uitzendbranche	Deze activiteit betreft structurele informatieaanvragen vanuit MKB inzake 'risicovolle' bedrijven in de uitzendbranche. Het doel is om inspecteurs van MKB om gericht te laten zoeken, door informatie aan te leveren van rechtspersonen in de uitzendbranche met een bepaald risicoprofiel. De eerstvolgende uitlevering staat ter discussie en wordt mogelijk niet uitgeleverd. Bij een eerstvolgende uitvraag vanuit MKB richting DF&A zal opnieuw een WIK-toets worden uitgevoerd en zullen voorwaarden worden opgesteld over hoe en welke data wordt aangeleverd. <i>Aangezien de uitlevering nog niet heeft plaatsgevonden (en de wijze waarop dit plaatsvindt) hebben wij niet kunnen vaststellen of het product voldoet aan de vereisten zoals is opgenomen in het overzicht van uit de managementsamen-vatting en dus de AVG, de Archiefwet en uw OA-kaders / Gouden Regels.</i>	De informatie ziet op rechtspersonen in de uitzendbranche die voldoen aan een bepaald risicoprofiel. De gegevens die verwerkt worden zijn vertrouwelijk op basis van het document 'Gouden Regels voor omgang met vertrouwelijke informatie'.	<i>Uitlevering van data heeft voorsnog niet plaats-gevonden dit jaar. Er zijn daarom geen risico's gedefinieerd.</i>	L

3. Detailoverzicht



*R = Risiconiveau

*Doc = Beschikbare documentatie

OB TELEFOONVERZUIM, [REDACTED]					
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
OB Telefoonverzuim	Algemeen kenmerken gegevensverwerking OB Telefoonverzuim is een lijst van alle starters van een onderneming die nog geen omzetbelastingaangifte hebben ingediend. Op deze lijst staan alleen ondernemers die de eerste aangifte nog niet hebben ingediend. Zij hebben namelijk één maand om de aangifte in te dienen. Hierna is er een coulanceperiode van zeven kalenderdagen. In die periode worden zij gebeld, aan de hand van de lijst. Het is dus geen toezichtproduct, maar een belijst. Medewerkers van [REDACTED] (klant-interactie) nemen contact op met de ondernemers om hen te wijzen op hun deadline. Het wordt gezien als serviceverlening. Er is momenteel geen feedback-loop terug naar DF&A – het is voor hen dus niet duidelijk wat het resultaat is. Als er verzuim optreedt, worden splitsingen gemaakt op basis van de persoonsgegevens genoemd in de volgende kolom, die de vervolgactie beslissen, namelijk of die persoon een brief ontvangt, of alleen gebeld wordt. Rechtmatige Grondslag: Valt onder de wettelijke taak van de Belastingdienst, het innen van belastingen. Doelbinding: Het primaire doel is het innen van belastingen en het doel dienstverlening. De verwerking is overeenkomstig deze doelstellingen. Gegevensuitwisseling derden: Er worden geen gegevens gedeeld met derden.	De betrokkenen zijn alle starters van een onderneming die de eerste OB-aangifte nog niet hebben ingediend. Als er verzuim is worden de volgende persoonsgegevens verzameld: OB-nummer, NAW, telefoonnummer, wanneer de aangifte binnen had moeten zijn, hoe vaak de ondernemer zijn belasting te laat heeft ingediend, is de persoon actief voor loonheffing, aanslagen niet betaald, teamnummer. Op basis daarvan worden splitsingen gemaakt: of de betrokkene wel of niet een brief krijgt, of alleen gebeld wordt. De persoonsgegevens zijn gevoelig volgens de definitie van de Gouden Regels, omdat het aangiftegegevens betreft. Ook kan het niet doen van aangifte een faillissement betekenen, wat het gevoelig maakt.	• Dataretentie: Er is geen bewaartermijn vastgesteld. Mogelijk worden gegevens langer bewaard dan noodzakelijk. • Proportionaliteit: Er heeft een beoordeling plaatsgevonden in een nog niet gefinaliseerde QC-toets en GEB over of de hoeveelheid gegevens in het overzicht beperkt blijft tot het strikt noodzakelijke. Hieruit bleek dat er verbetermogelijkheden zijn, die nog niet zijn doorgevoerd, omdat de documentatie nog niet gefinaliseerd is. • De query heeft naar aard en omvang een lage impact op eventuele risico's op non-compliance met AVG-standaarden. In dat verband vroegen enkele geïnterviewden zich af of de administratieve last van het uitvoeren van een volledige GEB en QC-toets wel opweegt tegen de geïdentificeerde privacyrisico's.	N	L

3. Detailoverzicht



*R = Risiconiveau

*Doc = Beschikbare documentatie

OB Tweeverzuim/Veelverzuim				
OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Algemeen kenmerken gegevensverwerking <i>Gelijk als OB Telefoonverzuim.</i> OB Tweeverzuim/veel verzuim is een lijst van alle starters van een onderneming die nog geen omzetbelastingaangifte hebben ingediend, en dit ook tweemaal of vaker hebben verzuimd. Het product die KINS (klantinteractie) gebruikt om startende ondernemers te bellen om hen eraan te herinneren om belastingaangifte te doen. Er is geen mogelijkheid voor een trigger in het primaire systeem dus wordt via een Excel-lijst als belijst vanuit DF&A verkregen. Rechtmatige Grondslag: Valt onder de wettelijke taak van de Belastingdienst, het innen van belastingen. Doelbinding: Het primaire doel is het innen van belastingen en dienstverlening. De verwerking is overeenkomstig deze doelstellingen. Gegevensuitwisseling derden: Er worden geen gegevens gedeeld met derden.	De betrokkenen zijn alle starters van een onderneming die twee- of driemaal hebben nagelaten om de OB-aangifte op tijd in te dienen. Als er verzuim is worden de volgende persoonsgegevens verzameld: OB-nummer, NAW, telefoonnummer, wanneer de aangifte binnen had moeten zijn, hoe vaak de ondernemer zijn belasting te laat heeft ingediend, is de persoon actief voor Loonheffing, aanslagen niet betaald, teamnummer. Op basis daarvan worden splitsingen gemaakt: of de betrokkene wel of niet een brief krijgt, of alleen gebeld wordt. De persoonsgegevens zijn gevoelig volgens de definitie van de Gouden Regels, omdat het aangifte-gegevens betreft. Ook kan het niet doen van aangifte een faillissement betekenen, wat het gevoelig maakt.	Proportionaliteit: Er heeft een beoordeling plaatsgevonden in een nog niet gefinaliseerde QC-toets en GEB over of de hoeveelheid gegevens in het overzicht beperkt blijft tot het strikt noodzakelijke. Hieruit bleek dat er verbetermogelijkheden zijn, die nog niet zijn doorgevoerd, omdat de documentatie nog niet gefinaliseerd is. Dataretentie: Er is geen bewaartemijn vastgesteld. Mogelijk worden gegevens langer bewaard dan noodzakelijk. - De query heeft naar aard en omvang een lage impact op eventuele risico's op non-compliance met AVG-standaarden. In dat verband vroegen enkele geïnterviewden zich af of de administratieve last van het uitvoeren van een volledige DPIA/GEB en QC-toets wel opweegt tegen de geïdentificeerde privacyrisico's.		L

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

WVK

WVK

GEB

GEB/AVG-scan

concept

for disclosure

*R = Risiconiveau
*Doc = Beschikbare documentatie

OB Bijzondere Normen, 				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEïDENTIFICEERDE RISICO'S	Doc* R*
OB Bijzondere Normen	Algemeen kenmerken gegevensverwerking OB Bijzondere normen heeft als doel om vervuiling van het OB systeem tegen te gaan en om datakwaliteit te garanderen. Ondernemers mogen maar een bepaalde omzetnorm terugvragen van de belastingdienst, die verschilt naar gelang de grootte van de onderneming. Ondernemers kunnen een bepaalde teruggavenorm toegewezen krijgen. Vanuit MKB wordt een uitvraag gedaan om twee lijsten, de afwijkende negatieve en positieve norm. DF&A vervaardigt een Excel-lijst door twee query's op het datafundament gebaseerd op het OB-systeem uit te voeren. Dit gebeurt ieder kwartaal. De lijst wordt vervolgens door MKB gebruikt om te verifiëren of de norm nog voor de onderneming van toepassing is of moet worden verwijderd om de datakwaliteit te borgen. De query-output wordt vervolgens in een Excel-bestand aangeleverd bij de van MKB. Dit gebeurt via 'ConnectPeople', waarvan alleen een ondernemingsmanager bij MKB en twee medewerkers van DF&A het wachtwoord en daarmee toegang hebben. De toegang tot het datafundament en de query is beperkt tot twee medewerkers van DF&A. De vervaardigde Excel-lijsten worden na overdracht aan MKB bewaard. Rechtmatige Grondslag: Valt onder de wettelijke taak van de Belastingdienst, het innen van belastingen. Doelbinding: Het primaire doel is het innen van belastingen en dienstverlening. De verwerking is overeenkomstig deze doelstellingen. Gegevensuitwisseling derden: Er worden geen gegevens gedeeld met derden.	De betrokkenen zijn ondernemingen die binnen de norm vallen. De uitvraag vindt viermaal per jaar plaats ten behoeve van datakwaliteit. Als er verzuim is worden de volgende persoonsgegevens verzameld: OB-nummer, welke norm betreft het, klant-segment/branche, team binnen BD, Belastingkantoor (overige gegevens). Proportionaliteit: Gezien het doel is de gegevensverwerking proportioneel. Uit de gesprekken blijkt dat er een WVK-toets beschikbaar is. De hebben wij echter niet ontvraagd.	- Er is geen bewaartermijn vastgesteld voor het bewaren van de Excel-lijst. Deze worden ook niet verwijderd. - Er is geen WVK-toets uitgevoerd en/of deze is niet aan ons ter beschikking gesteld. Dataretentie: Er is geen bewaartermijn vastgesteld. Mogelijk worden gegevens langer bewaard dan noodzakelijk.	
				M

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

WIK

WIK

GEB

GEB/AVG-scan

concept

discussie

*R = Risiconiveau
*Doc = Beschikbare documentatie

Branche informatie (Loondienst) Branche informatie (WIA en omzetbelasting) DFEK -152				
OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEïDENTIFICEERDE RISICO'S	Doc*	R*
Algemeen kenmerken gegevensverwerking <i>Branche-informatie Loondienst/WIA en omzetbelasting</i> Op de intranet pagina voor interne inspecteurs van de Belastingdienst is een informatiepagina waar onder het kopje 'Branche-informatie' de aangiften in het kader van Loondienst, WIA en OB met elkaar vergeleken kunnen worden per branche. In het overzicht worden geaggregeerde omzetcijfers op basis van de OB-aangiften uiteengezet zodat inspecteurs kunnen benchmarken met landelijke gemiddeldes. De informatie wordt per branchecode weergegeven op geaggregeerd niveau. Het doel is om de OB-aangiften per onderneming te kunnen vergelijken. Een overzicht van de gemiddeldes als referentiekader helpt daarbij. De output is een Excel-bestand met geaggregeerde gemiddelde kerngetallen per branche. Data wordt onttrokken uit één datafundament en vervaardigd door het medewerkers van het OSINT-team binnen DF&A. De output wordt gepubliceerd op Internetservice4U ten behoeve van de inspecteurs van MKB en kan niet worden gewijzigd of worden aangepast. Rechtmatige Grondslag: Valt onder de wettelijke taak van de Belastingdienst, toezichthouden. Doelbinding: Het doel is in lijn met het doel innen van belastingen en toezichthouden. Gegevensuitwisseling derden: Er worden geen gegevens gedeeld met derden. Dataretentie: Na aggregatie worden de gegevens vernietigd en voldoet daarmee aan het beginsel van opslagbeperking.	De betrokkenen zijn ondernemers. Persoonsgegevens worden geaggregeerd in het overzicht, dus zijn op basis van de overzichten niet herleidbaar tot individu. De ruwe data dat bestaat uit omzetcijfers van ondernemingen die mogelijk ook herleidbaar zijn tot informatie over inkomsten. Proportionaliteit: Wij hebben geen redenen om aan te nemen dat de gegevensverwerking niet proportioneel is ten opzichte van het gestelde verwerkingsdoel.	Geen risico's geïdentificeerd.	WIK	L

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

WIK

WIK

GEB

GEB/AVG-scan

concept

discussie

*R = Risiconiveau
*Doc = Beschikbare documentatie

FIOD Bijzondere Taken, geen DFEK –nummer aanwezig				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc* R*
FIOD Bijzondere Taken	Algemeen kenmerken gegevensverwerking Er zijn verschillend FIOD-afdelingen die DF&A verzoeken om informatie en advies. Deze FIOD-afdelingen hebben alle persoonsgegevens zelf in beheer. Het gaat hier niet om een structurele data-overdracht, maar het komt voor dat kennis gedeeld wordt op individueel niveau. Dit delen gaat niet via de mail of q-schijf; het is strikt geheim. Soms adviseert DF&A op ad-hoc basis welke gegevens gevorderd moeten worden bij andere instanties.	Voor het onderzoek dat DF&A uitvoert worden gewone en vertrouwelijke persoonsgegevens verwerkt die uit de bronssystemen komen. Hierbij worden geen bijzondere persoonsgegevens, bijvoorbeeld ten aanzien van etniciteit, verwerkt.	Dataretentie: Het is onduidelijk hoelang de persoonsgegevens worden bewaard - Er worden slechts incidenteel persoonsgegevens ingezien door DF&A, maar niet verder opgeslagen op systemen van DF&A. - Doordat er geen vastlegging is, kan ook geen verantwoording achteraf plaatsvinden.	M
	Rechtmatige Grondslag: Valt onder de wettelijke taak van de Belastingdienst van fraude opsporen en toezichhouden.	Proportionaliteit: Gezien de aard van de verstrekte persoonsgegevens (NAW-gegevens) is de gegevensverwerking proportioneel.		
	Doelbinding: Het doel is in lijn met het doel innen van belastingen en toezicht houden.			
	Gegevensuitwisseling derden: Er worden geen gegevens gedeeld met derden.			

3. Detailoverzicht

*R = Risiconiveau

*Doc = Beschikbare documentatie

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

MM

Minimo privacy risico's

WMK

Werk

GEB

GEB/AVG-scan



SIDN 				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEïDENTIFICEERDE RISICO'S	Doc* R*
SIDN	Algemeen kenmerken gegevensverwerking Artikel 53 lid 1 sub a AWR stelt de (inspecteurs van de) Belastingdienst in staat om gegevens op te vragen die van belang zijn voor de belastingheffing. Op grond van dit artikel vindt informatie-uitwisseling plaats tussen de Stichting Internet Domeinregistratie (SIDN) en de Belastingdienst. Er bestaat op grond van een convenant een geautomatiseerde interface 'Internet-service4u' tussen de database van SIDN en het intranet van de Belastingdienst. Middels een aanvraag in IMS kan toegang verkregen worden tot de interface. Medewerkers van team OSINT van DF&A zijn belast met de goedkeuring van deze aanvragen. De gebruikers en uitgevoerde zoekopdrachten worden periodiek gemonitord. De geretourneerde informatie vanuit SIDN wordt niet gelogd. Rechtmatige Grondslag: Valt onder de wettelijke taak van de Belastingdienst, toezichhouden. Doelbinding: Het doel is in lijn met het doel innen van belastingen en toezichhouden. Gegevensuitwisseling derden: Er worden geen gegevens gedeeld met derden. Dataretentie: Het is onduidelijk hoelang de persoonsgegevens worden bewaard.	SIDN verstrekt via de koppeling naar het internet van de Belastingdienst contactinformatie van de natuurlijke persoon die de domeinnaam bij SIDN heeft geregistreerd. Het gaat hierbij om telefoonnummer, e-mailadres en woonadres. Daarnaast worden de domeinnaam en het bijbehorende IP-adres verwerkt en verstrekt aan de Belastingdienst. Proportionaliteit: Gezien de aard van de verstrekte persoonsgegevens (NAW-gegevens) is de gegevensverwerking proportioneel.	- Geïnterviewde gaf aan dat de datakwaliteit van het register van SIDN niet altijd betrouwbaar en actueel is. De geretourneerde informatie vanuit SIDN wordt niet gelogd. Dit geeft het risico dat onjuiste persoonsgegevens worden verwerkt. - Het is onduidelijk hoelang de persoonsgegevens worden bewaard.	WMK MM L



3. Detailoverzicht Categorie 3*

*Er worden (veel) persoonsgegevens verwerkt en/of er is sprake de verwerking van (veel) gevoelige of bijzondere persoonsgegevens of waarbij sprake is van een hoog risico verwerkingsactiviteit, zoals profilering

3. Detailoverzicht

*R = Risiconiveau

*Doc = Beschikbare documentatie

H Risiconiveau Hoog MM Memo privacy risico's
M Risiconiveau Midden WVK WVK
L Risiconiveau Laag GEB GEB/AVG-scan

concept discussie!

DAS-tool,					
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
DAS-tool	Algemeen kenmerken gegevensverwerking De DAS tool heeft als doel het nabootsen van de loonaangifte om de oorzaak van fouten op te kunnen sporen. Hierbij maakt de DAS-tool gebruik van de XML-berichten die in het DAS-archief worden opgeslagen. De bron van de gegevens is de werkgever zelf, via de aangiftes. Wanneer een gegeven in het klantsysteem niet klopt, dan krijgt een werkgever een brief. Bijvoorbeeld dat voor een werknemer het BSN of de geboortedatum onjuist is. Gegevensuitwisseling derden: In het kader van analyseren, kent de DAS-tool twee omgevingen. De eerste is het voornoemde DAS-archief waar aangiftes staan. De tweede omgeving is de poort naar het UWW waardoor de polis van een werkgever te benaderen is en kan worden vergeleken. AGL is een samenwerking tussen de Belastingdienst en UWW waarbij om de zoveel tijd bestanden worden vergeleken om verschillen op te kunnen sporen. Proportionaliteit: Gezien de aard van de verstrekte persoonsgegevens (NAW-gegevens) lijkt de gegevensverwerking proportioneel ten opzichte van het gestelde verwerkingsdoel. Een middel hiertoe is de zgn. kruisjeslijst van het UWW, die bepalend in wat niet opgenomen mag worden in een uitdraai/export. Deze kruisjeslijst is de lijst met gegevens waarvan het UWW zegt dat die niet nodig zijn voor (verdere) verwerking. Zo is bijvoorbeeld het opgebouwd vakantiegeld op deze kruisjeslijst gezet. Rechtmatige grondslag: Valt onder de wettelijke taak van de Belastingdienst, toezichthouden.	Betrokkenen: werkgevers, werknemers, fiscale partners van belastingplichtigen, uitsluitend t.a.v. de loonaangifte en polissen. Periodiek wordt een beeld opgevraagd van een polis en de daarmee samenhangende technische sleutels. Een dergelijke technische sleutel (hash-key/totaal-key) is een samenvoegsel van onder meer het BSN, LH-nummer, numerieke inkomstenverhoudingsnummer, werknemersnummer en de periode van opvraging. Verder worden de hoogte van loon en premiekorting verwerkt. Er worden geen bijzondere persoonsgegevens verwerkt. Ook zijn er geen medische gegevens af te leiden uit de gegevens, bijvoorbeeld door bepaalde premiekortingen die verband kunnen houden met ziekte zoals de WIA of Wajong.	Dataretentie: Het eigenaarschap over het voldoen aan AVG-normen wordt middels een disclaimer bij de eindgebruiker gelegd. Voldoen aan bewaartermijnen ligt enerzijds bij de eindgebruiker, en anderzijds bij eigenaren van het DAS-archief. Doelbinding: met betrekking tot de doelbinding bestaat een drietal risico's: - Een risico dat in de GEB wordt omschreven is die van doelbinding, gezien gearchiveerde gegevens worden verwerkt, wat in strijd is met het doel van archiveren conform de archiefwet. - Daarnaast is een belangrijk risico uit de GEB dat de risicoprofieling als zwarte lijst gaat gelden en een eigen leven gaat leiden, buiten de geformuleerde opdracht om. - DF&A-medewerkers kunnen de fiscale gegevens van alle loonbelastingplichtigen inzien. Logging en monitoring vindt plaats door het centrale SOC-team op de test- en ontwikkelomgeving, maar niet op het gebruik door eindgebruikers. Het risico is dat loongegevens onrechtmatig worden verwerkt door eindgebruikers en/of geëxporteerd en (extern) gedeeld kunnen worden.	GEB MM	M

3. Detailoverzicht

*R = Risiconiveau

*Doc = Beschikbare documentatie

H Risiconiveau Hoog MM Memo privacyrisico's
M Risiconiveau Midden WNK WNK
L Risiconiveau Laag GEB GEB/AVG-scan

Zeer vermogende personen, [REDACTED]				
OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Algemeen kenmerken gegevensverwerking Het programma [1] heeft als doel om de eigenaren van grote bedrijven in Nederland inzichtelijk te maken en te rangschikken naar bezit en schulden. Enerzijds heeft het programma het doel om belastingfraude op te sporen. Anderzijds heeft het programma een signaalfunctie op het gebied van erf- en schenkrecht. De data wordt vervaardigd door een query uit te oefenen op een database, waarna deze wordt vormgegeven in een Excel-bestand en middels een interne fileshare wordt gedeeld met GO (Grote Ondernemingen?). De inspecteurs van GO voeren vervolgens aan de hand van deze informatie hun onderzoeken uit. De frequentie van het opstellen en aanleveren van deze informatie is twee keer per jaar. Het overzicht wordt samengesteld op (een kopie van) een database via SQL-query's en SAS-scripts. Deze query's worden opgeslagen in een folder binnen de Teradata Datawarehouse. Deze query's zijn niet afgeschermd. Er vindt momenteel een migratie plaats naar een dedicated database waarbij dit wel afgeschermd zal zijn. De query-output wordt vervolgens in een Excel-bestand aangeleverd bij de [REDACTED] van GO. Dit gebeurt via 'Connect-People', waarvan alleen één GO- en één DF&A [REDACTED] het wachtwoord en daarmee toegang hebben. Rechtmatige grondslag: Wij hebben niet kunnen vaststellen wat de wettelijke grondslag is en of deze rechtmatig is als zodanig. Doelbinding: Het doel is in lijn met één van de hoofddoelen van de Belastingdienst, toezicht houden. Gegevensuitwisseling derden: Er worden geen gegevens gedeeld met derden. Dataretentie: De lijst wordt na overdracht meteen verwijderd en voldoet daarmee aan het beginsel van opslagbeperking.	De betrokkenen zijn natuurlijke personen die kwalificeren als zeer vermogend inclusief diens fiscale partner en de overige leden van diens huishouden. Persoonsgegevens die verwerkt worden zijn: BSN, financiële informatie zoals saldi lopende rekeningen, saldi spaarrekeningen, schulden, giften, schenkingen, geldstromen binnen de B.V., informatie omtrent vermogen (vastgoedobjecten en BV's), fiscaal partnerschap, informatie omtrent de samenstelling van het huishouden. Proportionaliteit: Er [REDACTED] geen GEB te zijn uitgevoerd. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	- De code is inzichtelijk voor andere medewerkers van DF&A - Meerdere collega's hebben mogelijk toegang tot de code. - Wij hebben niet kunnen vaststellen wat de wettelijke grondslag is. [2] - Er is geen GEB uitgevoerd en/of deze is niet aan ons ter beschikking gesteld. - De verwerking voldoet mogelijk niet aan het beginsel van proportionaliteit.		H

Pagina: 25

	Nummer: 1	Auteur:	Onderwerp: Notitie Datum: 25-11-2020 15:21:12 +01'00'
	Omschrijving klopt niet. Het gaat om individuele klantbehandeling van de top-1500 zeer vermogende personen. Zie toegevoegde documentatie op CP. Incl. intranet bericht: https://intranet.belastingdienst.nl/nieuws/2020/06/15/programma-zeer-vermogende-persoon-en-richt-zich-op-1-500-rijkste-families/		
	Nummer: 2	Auteur:	Onderwerp: Notitie Datum: 25-11-2020 15:22:12 +01'00'
	Wel een WMK. Grondslag is ook bekend! Aanpak is ook proportioneel.		
	Nummer: 3	Auteur:	Onderwerp: Notitie Datum: 25-11-2020 15:21:25 +01'00'
	Is er allemaal wel.		

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Middel

L

Risiconiveau Laag

MM

Minimale privacyrisico's

WMK

Wettelijke Medische Keuring

GEB

GEB/AVG-convenant

Concept

for discussion

*R = Risiconiveau

*Doc = Beschikbare documentatie

Directoraat-Generaal Fiscale Zaken				
OMSCHRIJVING EN DOEL VAN DE VERWERKING		SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc* R*
Directoraat-Generaal voor Fiscale Zaken	Algemeen kenmerken gegevensverwerking  1 Het Directoraat-Generaal Fiscale Zaken betreft een apart gebied op het analytics-platform van DF&A waarbij analisten van de Ministerie van Financiën toegang wordt verstrekt tot de gehele dataset van DF&A. De datasets strekken tot de maximaal drie voorafgaande jaren. Data-uitwisseling gebeurt op grond van een convenant met het Ministerie van Financiën. Wij hebben geen documenten ontvangen. Wij hebben op basis van de gesprekken niet kunnen vaststellen of en in welke mate het product voldoet aan de gestelde eisen. Het is onbekend of dit product nog in werking is. Rechtmatige grondslag: Wij hebben niet kunnen vaststellen wat de wettelijke grondslag is en of deze potentieel grootschalige verwerking als zodanig rechtmatig is. Doelbinding: Het doel is in lijn met één van de hoofddoelen van de Belastingdienst, namelijk toezichthouden. Gegevensuitwisseling derden: Er worden gegevens uitgewisseld met het Ministerie van Financiën op basis van een convenant. Dataretentie: Er wordt real-time gegevens ter inzage gesteld aan de analisten van het Ministerie.	Financiële gegevens (inkomsten, schulden, banktransacties, etc.) tot aan persoonsniveau. Proportionaliteit: Er lijkt geen GEB te zijn uitgevoerd. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	- Er wordt brede toegang tot alle datasets van DF&A verleend aan Financiën. - Wij hebben niet kunnen vaststellen wat de wettelijke grondslag is. - Er is geen GEB uitgevoerd en/of deze is niet aan ons ter beschikking gesteld. Daarnaast hebben wij geen inzage gehad in het convenant op basis waarvan gegevensoverdracht plaatsvindt. - De verwerking voldoet mogelijk niet aan het beginsel van proportionaliteit.	H

 Nummer: 1 Auteur: Onderwerp: Notitie Datum: 25-11-2020 15:23:26 +01'00'

Is dit een oud-EH&I product? Volgens mij hebben ze geen toegang tot alle data of wel? SVP checken bij team data e.d.

3. Detailoverzicht

*R = Risiconiveau

*Doc = Beschikbare documentatie

H

Risiconiveau Hoog

M

Risiconiveau Middel

L

Risiconiveau Laag

MM

Memo privacyrisico's

WKK

Wettelijke Kern

GEB

GEB/AVG-scan

Concept
for discussion

Gruff Netwerkanalysetool				
OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Algemeen kenmerken gegevensverwerking Gruff is een visualisatietool die als interface draait op een AllegroGraph-database. De visualisatietool wordt gebruikt om bepaalde netwerken en verbanden visueel inzichtelijk te maken. Medewerkers van vrijwel alle onderdelen van de Belastingdienst kunnen hiervan gebruikmaken, mits de tool wordt gebruikt in het kader van de landelijke fraudebestrijding en toezicht. De tool zelf is niet in gebruik genomen met een verwerkingsdoel. De verantwoordelijkheid voor het doel van de betreffende verwerking is belegd bij de gebruiker (er kunnen door gebruikers verschillende verwerkingen worden toegepast, niet noodzakelijkerwijs allemaal met hetzelfde verwerkingsdoel). Medewerkers kunnen via hun [] toegang aanvragen tot Gruff via het IMS-autorisatiesysteem. Twee medewerkers van DF&A zijn belast met de beoordeling van deze autorisatie-aanvragen. De eis waaraan getoetst dient te worden is of de tool zal worden gebruikt in het kader van de landelijke fraudebestrijding en -toezicht. De onderliggende AllegroGraph-database bevat kopieën van brondata uit het Handelsregister en uit interne bronnen. Er wordt eenmaal per een à twee weken opnieuw een query gedraaid op het bronsysteem. Gebruikers van de tool worden er met de voorwaarden op gewezen dat de gegevens uit de database niet meer actueel kunnen zijn en dat de brondata zelf te allen tijde geraadpleegd dient te worden. Rechtmatige grondslag/doelbinding: het gebruikende Belastingdienstonderdeel is verantwoordelijk voor het verwerken met een wettelijke grondslag en in lijn met het gedefinieerde doel, zoals bijvoorbeeld de wettelijke taak van toezichthouden. Gegevensuitwisseling derden: Er worden geen persoonsgegevens uitgewisseld. Datarententie: Het is onduidelijk hoelang de persoonsgegevens worden bewaard.	De datasubjecten betreffen natuurlijke personen inclusief fiscale partner en overige leden van het huishouden. De verwerking ziet op het aantonen van verbanden en netwerken tussen personen en bedrijven. De soorten persoonsgegevens die opgeslagen zijn in de AllegroGraph-database zijn divers door de verschillende bronnen die worden gecombineerd (handelsregister en interne bronnen). Proportionaliteit: Er lijkt geen GEB te zijn uitgevoerd, er is wel een memo over privacyrisico's opgesteld. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	- Binnen DF&A is geen verwerkingsdoel bepaald voor het gebruik deze tool. Deze verantwoordelijkheid is belegd in de lijnorganisatie. Op deze manier is het niet mogelijk om te toetsen of de verwerking nog in lijn is met het oorspronkelijke doel. Dit is tevens van belang om de proportionaliteit en de subsidiariteit van elke verwerking te kunnen bepalen. - In de database is het mogelijk om "VIP's" te identificeren. Hier wordt geen rekening mee gehouden bij het toekennen van autorisaties. Wel wordt dit risico gemitigeerd doordat er monitoring plaatsvindt op het gebruik. Eenmaal per maand wordt aan de FG een overzicht aangeleverd van de logging wat betreft het gebruik van Gruff, inclusief welke BSN's geraakt zijn en of er VIP's zijn geraakt en door wie. - Er is geen GEB uitgevoerd [] en/of deze is niet aan ons ter beschikking [] gesteld. - De verwerking voldoet mogelijk niet aan het beginsel van proportionaliteit. - Mogelijk worden persoonsgegevens te lang bewaard.	WKK MM	M H

Gruff Netwerkanalysetool

 Nummer: 1 Auteur: Onderwerp: Notitie Datum: 25-11-2020 15:31:00 +01'00'

Voor maar ook veelverzuim en andere producten zijn verkorte PIA's uitgevoerd door Deze zijn behandeld in het MT op 28-5-2019

3. Detailoverzicht

H Risiconiveau Hoog MM Memo privacyrisico's
M Risiconiveau Middel WVK WVK
L Risiconiveau Laag GEB GEB/AVG-Beaan

*R = Risiconiveau
*Doc = Beschikbare documentatie

Concept
for discussion

Marktplaatsverzoek						
OMSCHRIJVING EN DOEL VAN DE VERWERKING		SOORT PERSOONSgegevens EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*	
Marktplaatsverzoek	Algemeen kenmerken gegevensverwerking Artikel 53 lid 1 sub a AWR stelt de (inspecteurs van de) Belastingdienst in staat om gegevens op te vragen die van belang zijn voor de belastingheffing. Op grond van dit artikel en een onderling convenant vindt informatie-uitwisseling plaats tussen Marktplaats en de Belastingdienst. Deze procedure verloopt niet geautomatiseerd, maar via DF&A. DF&A krijgt verzoeken inzake natuurlijke personen van onderdelen die belast zijn met het doen van onderzoek naar deze personen. Deze verzoeken worden samengevoegd in een overzicht en opgestuurd naar Marktplaats via de Belastingdienst filetransfer. DF&A ontvangt vervolgens de resultaten in een standaardformaat op de Belastingdienst filetransfer. Vervolgens zet DF&A het bestand met de resultaten intern weer uit via Connectpeople. DF&A fungeert hierbij derhalve slechts als 'doorgeefluik'. De inspecteur (van MKB of P) die deze persoonsgegevens via DF&A bij Marktplaats aanvraagt dient een rechtmatige grondslag te hebben en de gegevens derhalve adequaat en conform de AVG te verwerken. Alleen de informatie omtrent verzoeken aan Marktplaats worden opgeslagen binnen DF&A. De resultaten die de Marktplaats aanlevert, worden direct verwijderd door de medewerker van het OSINT-team.		Er worden persoonsgegevens aangeleverd van de gebruiker van Marktplaats. Het standaardformaat waarin Marktplaats de informatie aanlevert bevat de volgende gebruikersgegevens: Gebruikers-ID en -naam, e-mailadres, IP-adres, NAW-gegevens, informatie over het betaalgebruik van de gebruiker (indicatie gebruik Paypal) en informatie over de door de gebruiker geplaatste advertentie(s). Proportionaliteit: Er lijkt geen GEB te zijn uitgevoerd, er is wel een memo over privacyrisico's opgesteld. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	- Het is onduidelijk hoelang de registratie van de natuurlijke personen waarvoor de Belastingdienst een verzoek indient bij Marktplaats wordt opgeslagen. - Mogelijk worden de advertentiegegevens van leden van het huishouden van de natuurlijke persoon waarnaar onderzoek wordt gedaan verwerkt. - Er is geen GEB uitgevoerd en/of deze is niet aan ons ter beschikking gesteld. - De verwerking voldoet mogelijk niet aan het beginsel van proportionaliteit.	WVK MM M	
	Rechtmatige grondslag/doelbinding: het gebruikende Belastingdienstonderdeel is verantwoordelijk voor het verwerken met een wettelijke grondslag en in lijn met het gedefinieerde doel, zoals bijvoorbeeld de wettelijke taak van toezichthouden.					
	Gegevensuitwisseling derden: Er worden geen persoonsgegevens gedeeld met derden.					
	Dataretentie: Het is onduidelijk hoelang de persoonsgegevens worden bewaard.					

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

WMK

WMK

GEB

GEB/AVG-scan

concept

discussie

*R = Risiconiveau
*Doc = Beschikbare documentatie

FIOD Berlijn trailer, geen DFEX -nummer				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEïDENTIFICEERDE RISICO'S	Doc* R*
FIOD Berlijn trailer	Algemeen kenmerken gegevensverwerking Het viel DF&A op dat veel signalen vanuit het buitenland betrekking hadden op voertuigen die werden geëxporteerd naar Oost-Europa. Dat was de trigger om het nader te onderzoeken. Dit heeft ertoe geleid dat een grote fraudezaak geconstateerd kon worden. Dit was aanvankelijk een eenmalige analyse, maar inmiddels wordt deze elke drie maanden herhaald. De analyse wordt op data vanuit de organisatie (MKB en GO) gedaan, waarbij personen van DF&A worden ingehuurd. Het doel van 'FIOD Berlijn trailer' is de preventie van fraude.	De gegevens die voor deze analyse worden gebruikt zijn in beheer van FIOD en betreffen gegevens over vastgoed, lonen en auto's, aangiften en KvK-gegevens (handelsregisters), zoals het bezitten van ontbonden rechtspersonen, de status van de afnemer en diens nationaliteit.	Deze tak van DF&A lijkt op R&D, wat niet belegd is. Er zou een besloten kring moeten zijn van mensen die toegang tot deze data zou moeten hebben, maar die is niet bepaald. Op het moment dat DF&A zelf risicosignalen gaat identificeren, is het risico dat een opdrachtgever en daarmee een risico-eigenaar ontbreekt. Er wordt elke drie maanden data geleverd aan MKB, zonder dat hiervoor een WMK, QC en/of GEB over is uitgevoerd. Ook heeft deze data-uitlevering geen DFEX-nummer, waardoor het niet traceerbaar is, bijvoorbeeld voor de [] Gegevens worden gedeeld via de mail, wat in strijd is met de gouden regels. Gegevens aan een algemeen mailadres kunnen niet versleuteld worden. Dataretentie: Een retentietermijn is niet vastgelegd of geformaliseerd. Enerzijds is historie noodzakelijk om tendensen te kunnen bepalen. Ook op individueel niveau komt het voor dat een veelpleger na zes jaar weer naar boven komt. Dan is het noodzakelijk de historische data te hebben. Anderzijds moet een bewaartermijn beredeneerd vastgesteld kunnen worden. Op dit moment is niet duidelijk wat wel en wat niet bewaard hoeft te worden.	N H
	Rechtmatige grondslag/doelbinding: het gebruikende Belastingdienstonderdeel is verantwoordelijk voor het verwerken met een wettelijke grondslag en in lijn met het gedefinieerde doel, zoals bijvoorbeeld de wettelijke taak van toezichthouden. Gegevensuitwisseling derden: Informatie wordt niet extern gedeeld door DF&A. Informatie kan via de officiële lijn van CPB wel extern, bijvoorbeeld de politie, gedeeld worden.	De scope van betrokkenen zijn niet beperkt tot de EU, maar kan alle mogelijk frauderende personen betreffen. Met name houders van rechtspersonen, zoals Leasebedrijven. Proportionaliteit: Er lijkt geen GEB te zijn uitgevoerd. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.		

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

WMK

WMK

GEB

GEB/AVG-scan

concept

discussie

*R = Risiconiveau
*Doc = Beschikbare documentatie

FIOD Centraal punt BTW-fraude, geen DFEX –nummer aanwezig					
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
FIOD Centraalpunt BTW-fraude	Algemeen kenmerken gegevensverwerking FIOD Centraalpunt BTW-fraude was een eenmalige analyse naar aanleiding van auto's die met cash-gelden zijn betaald. Momenteel wordt deze analyse elke drie maanden herhaald. De analyse wordt gedaan op basis van data afkomstig uit de organisatie (samenwerkingsverband tussen MKB en FIOD). Als de organisatie verdachte signalen ziet, wordt dit gemarkeerd. Vervolgens komt dit terecht bij DF&A ter advisering inzake fenomenen. Na een mogelijke combinatie van risico verhogende indicatoren die vermoedelijk wijzen op fraude, dient vervolgens vanuit een gefaseerde aanpak gepaard te gaan met een extra uitvraag van relevante informatie. Dit kan vervolgens leiden tot strafrechtelijk onderzoek naar diverse personen, zoals bijvoorbeeld fraude-faciliterende notarissen. In het kader van de handel in auto's kan als indicator gedacht worden aan contante betalingen. Het doel is grootschalige veelvoorkomende fenomenen tegengaan die naar aard en omvang een grote financiële impact hebben. DF&A is hierbij ondersteunend aan de organisatie. Rechtmatige grondslag: Het is aannemelijk dat deze verwerking past bij de wettelijke taak van de Belastingdienst, namelijk toezichthouden. Doelbinding: Het is aannemelijk dat het verwerkingsdoel past binnen één van de hoofddoelen van de Belastingdienst, namelijk toezichthouden. Gegevensuitwisseling derden: DF&A deelt geen persoonsgegevens met derde partijen – wel kennis.	Centraal punt BTW-fraude specialiseert zich in fraude binnen de lidstaten van de EU. Betrokkenen kunnen houders van rechtspersonen, zoals houders van leasebedrijven zijn, of frauduleuze notarissen. Er worden reguliere persoonsgegevens verwerkt, en vertrouwelijke persoonsgegevens Er worden geen bijzondere persoonsgegevens verwerkt. Inzage in de nationaliteit is wel mogelijk. In het geval van een immigrant wordt bijvoorbeeld gekeken of hij/zij non-compliant is in de lidstaat waar die van afkomstig is. Het samenstel van factoren/indicatoren kan leiden tot een verhoogd risicoprofiel. Proportionaliteit: Er lijkt geen CEB te zijn uitgevoerd. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	Dataretentie: Het is onduidelijk hoelang de persoonsgegevens worden bewaard. Er wordt elke drie maanden data geleverd aan MKB, zonder dat hiervoor een WMK, QC en/of GEB over is uitgevoerd. Ook heeft deze data-uitlevering geen DFEX-nummer, waardoor het niet traceerbaar is, bijvoorbeeld voor de Het eigenaarschap van het laten bestaan van dergelijke documentatie wordt niet erkend door DF&A-leden, maar wordt geacht bij de organisatie te liggen. Deze vorm van fraudepreventie is uitermate gevoelig, maar de need-to-know van deze gegevens is niet omschreven. Er zou wel geanonimiseerd of gepseudonimiseerd kunnen worden nadat de analyse is voltooid. Dat gebeurt nu echter niet.	N	H

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

WIK

MKB

GEB

GEB AVG-scan

concept

discussie

*R = Risiconiveau
*Doc = Beschikbare documentatie

FIOD – AMLC (Trade based money laundering; FIU; No Shelter), geen DFEK-nummer aanwezig				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEïDENTIFICEERDE RISICO'S	Doc* R*
FIOD – AMLC (Trade based money laundering; FIU; No shelter)	Algemeen kenmerken gegevensverwerking Dit betreft een kennisdeling van DF&A met FIOD ten aanzien van witwassen, bijvoorbeeld het detecteren van risicovolle adressen en trustkantoren. DF&A analyseert hier FIOD-gegevens, aangevuld met eigen bronbestanden van DF&A. Het gaat hier vaak om mensen die geen wilsovertuiging hebben, maar handelen in opdracht van een ander.	In aanvulling op andere FIOD producten wordt hier gekeken naar bankmutaties. Deze mutaties worden opgevraagd bij de banken door MKB waarbij FIOD hierover advies geeft.	Dataretentie: Het is onduidelijk hoelang de persoonsgegevens worden bewaard. De processen rondom dit product is niet formeel in documentatie vastgelegd, en niet getoetst. Het is daardoor lastig aantoonbaar te maken dat persoonsgegevens van deze processen op een veilige manier verwerkt worden.	M
	Gegevensuitwisseling derden: Via de officiële lijnen kunnen gegevens niet rechtstreeks met derde partijen worden gedeeld. Er is enkel sprake van het intern delen van gegevens. Eventueel kunnen gegevens terecht komen bij een intern onderdeel dat wel bevoegd is tot het extern delen van gegevens, en via die weg intern gaan. Dit is een afweging die buiten DF&A ligt.	Betrokkenen vloeien voort uit de data flows die samenhangen met grootschalige fraude/misbruik. Specifiek komen de betrokkenen onder meer neer op: notarissen en houders van rechtspersonen.		
	Rechtmatige grondslag/doelbinding: het gebruikende Belastingdienst-onderdeel is verantwoordelijk voor het verwerken met een wettelijke grondslag en in lijn met het gedefinieerde doel, zoals bijvoorbeeld de wettelijke taak van toezichthouden.	Proportionaliteit: Er lijkt geen GEB te zijn uitgevoerd. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.		

3. Detailoverzicht

H

Risiconiveau Hoog

M

Risiconiveau Midden

L

Risiconiveau Laag

Wmk

Wmk

GEB

GEB/AVG-scan

concept

for disclosure

*R = Risiconiveau
*Doc = Beschikbare documentatie

Veelplegers team (nieuwe naam: Team aanpak risicovolle netwerken), geen DFEK –nummer aanwezig				
OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Algemeen kenmerken gegevensverwerking DISCLAIMER: Het werd ons niet geheel duidelijk wat de rol van DF&A t.o.v. dit nieuwe team is. Graag ontvangen we nog informatie hierover. In het verleden werden eenmalige analyses op aanvraagbasis aan het veelplegers-team geleverd. Die zijn niet meer in productie. De naam van het team is inmiddels gewijzigd naar het Team aanpak risicovolle netwerken. Het viel op dat er bepaalde soorten fraude vaak voorkwam. Toen is aanvankelijk een project gestart. Momenteel is een speciaal team in Zwolle dat zich richt op natuurlijke personen en rechtspersonen binnen netwerken ter voorkoming van fraude, het direct stoppen van fraude, en aansprakelijkstelling om gelden terug te kunnen krijgen. DF&A voert analyses uit voor dit team op basis van eigen bronnen en de KvK. Bij bepaalde signalen zoals bijvoorbeeld turboliquidaties (wanneer een BV binnen vier maanden wordt geliquideerd) kan het gaan om dezelfde personen (veelplegers). De noodzaak om terug te gaan naar historische data is dan aanwezig, vooral wanneer sprake is van veelplegers en non-complianten. Het huidige gedrag is leidend, waarbij de wisseling van bestuurders en aandeelhouders bijvoorbeeld een 'red flag' kunnen zijn. Rechtmatige grondslag/doelbinding: het gebruikende Belastingdienst-onderdeel is verantwoordelijk voor het verwerken met een wettelijke grondslag en in lijn met het gedefinieerde doel, zoals bijvoorbeeld de wettelijke taak van toezichthouders. Gegevensuitwisseling derden: Er worden geen persoonsgegevens gedeeld met derden.	De betrokkenen zijn mogelijk fraudeurs, zowel bewuste als onbewust. De gegevens zijn afkomstig uit eigen bronnen van DF&A en de KvK. Hierbij kan gedacht worden aan de volgende persoonsgegevens: NAW-gegevens, BSN, IP, e.d. Proportionaliteit: Er is wel een GEB voor het Veelplegers team uitgevoerd, alleen komt de DF&A-rol hierin niet naar voren. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	Dataretentie: Het is onduidelijk hoelang de persoonsgegevens worden bewaard. Evt. nog aangevuld met andere risico's als ontbrekende informatie beschikbaar komt.	N	H

 Nummer: 1 Auteur: Onderwerp: Notitie Datum: 25-11-2020 15:34:03 +01'00'

Dit hangt samen met de signaalpostbus. SVP over doorpraten

3. Detailoverzicht

*R = Risiconiveau

*Doc = Beschikbare documentatie

 Risiconiveau Hoog

 Risiconiveau Midden

 Risiconiveau Laag


Signaalanalyse postbus, geen DFEX –nummer aanwezig				
OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSgegevens EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Algemeen kenmerken gegevensverwerking DISCLAIMER: Het werd ons niet geheel duidelijk welke precieze rol DF&A heeft t.a.v. dit product. We zouden documentatie ontvangen, maar hebben deze niet gekregen. Het betreft het Memo inzake fraudesignalen en twee procesplaten (signaalanalyse en fraudepreventie) over de aanpak. Graag ontvangen wij nog extra informatie hierover. Voorheen werden alle interne en externe fraudesignalen die binnenkwamen op de Signaalanalyse postbus opgewerkt en doorgezet. Momenteel gebeurt dit echter alleen met het externe signaal dat van Track Justis afkomstig is. Informatieverzoeken die van Track Justis binnenkomen gaan rechtstreeks naar CAP, waar deze worden vastgelegd. Vervolgens komt het verzoek aan DF&A om de gegevens aan te vullen met benodigde informatie, zodat Track Justis de strafrechtelijke behandeling kan voortzetten. Analisten van DF&A vullen de gegevens aan met reguliere bestanden, zoals boekenonderzoeken. Als de set compleet is, gaat het vanuit de Signaalanalyse postbus terug naar Track Justis. Zij gaan er vervolgens samen met andere informatie vanuit de politie een risicoprofiel of melding van opmaken. Track Justis heeft vanuit het Ministerie van JenV de opdracht om de Wet op de ondernemingen uit te voeren. Ze toetsten of ondernemingen mogen worden gestart. Op basis van een convenant kan informatie bij de Belastingdienst worden opgevraagd. DF&A gebruikt het signaal van het informatieverzoek vervolgens om advies te geven aan het team aanpak en risicovolle netwerken dat ze mogelijke niet naleving (non compliance) kunnen verwachten. Zo pogen ze aan de voorkant de mogelijkheid tot niet-naleving z.s.m. te signaleren. Gegevensuitwisseling derden: Dit gebeurt op basis van het convenant. Datarententie: Zonder sommige historische data (b.v. IP-adressen) is het niet mogelijk fraude op te sporen noch tegen te gaan. Verzoeken van Track worden twee jaar bewaard en daarna opgeschoond.	De betrokkenen betreffen mensen van wie door Track Justis een informatieverzoek aan Belastingdienst wordt gedaan. De persoonsgegevens die worden verwerkt, komen voornamelijk uit eigen systemen/bronnen en die van de Kamer van Koophandel. Hierbij kunnen aangiftegegevens, gegevens over geldstromen, nationaliteit en verblijfstitel verwerkt worden. Soms wijzen feiten op het internet in de vorm van fraude meldingen in de richting van veelplegers. Proportionaliteit: Het is niet duidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	Gegevens worden per mail gedeeld, terwijl deze niet versleuteld kunnen worden, gezien het een algemeen emailadres betreft. Er is een risico dat de grondslag en doelbinding voor het secundaire gebruik ontbreekt. Doelbinding: Het primaire doel van beantwoorden van informatieverzoeken is in lijn met het doel van het convenant. Het secundaire doel waarin signalen door worden gezet naar Team Aanpak Risicovolle Netwerken geschiedt niet op basis van dit convenant, maar heeft een algemener doel van fraude-opsporing en preventie. Rechtmatige grondslag: Het beantwoorden van informatieverzoeken valt onder het convenant tussen onder andere Track Justis en de Belastingdienst. Het verder verwerken van deze gegevens valt hier niet onder. Het risico bestaat dat voor deze verwerking er geen grondslag is. Ext. nog aangevuld met andere risico's als ontbrekende informatie beschikbaar komt.	N	M

 Nummer: 1 Auteur: Onderwerp: Notitie Datum: 25-11-2020 15:36:10 +01'00'

Ook hiervoor is een verkorte PIA uitgevoerd.



Appendices

Appendix A – Lijst van interviews

Appendix B – Bestudeerde documentatie



Appendix A – Lijst van interviews



Wij hebben ten behoeve van het onderzoek onderstaande interviews gehouden.

Onderwerpen	Datum
Zeer Vermogende Personen	21 oktober 2020
[] - Netwerkanalyse tool inclusief data; SIDN; Marktplaatslevering/marktplaatsverzoeken; Brancheinformatie (loondienst) Brancheinformatie (omzetbelasting en WIA); Intranetportal/Service 4u.	22 oktober 2020
[] EOS; Fraude EOS teams; Fraude teams Particulieren; Fraude deskundigenoverleg (FDO); Manifestgroepfraude; Werkgroep RUB (risicovolle uitbetalingen) CAP; Werkgroep faillissementsfraude (Min van J&V).	28 oktober
Schoonmaakbranche Uitzendbranche Schijnconstructies	29 oktober

Onderwerpen	Datum
FIOD account; FIOD Berlijn – Trailer; FIOD Centraalpunt BTW-fraude; FIOD strategische opsporingsinformatie; FIOD centraal punt faillissementsfraude; FIOD – AMLC - Trade based money laundering - FIU - No shelter; FIOD Acquisitie; FIOD Bijzondere Taken; FIOD IFFC Trendwatchingrapport Radicaal Samenwerken waarbij op basis van interviews (leidt tot externe publicatie; Veelplegers team; Voorlichting en Training Notariaat (KNB; extern); Werkgroep faillissementsfraude (Min van J&V).	3 en 11 november
QA/QC-raamwerk; DPIA/GEB-proces.	4 november 2020
Telefoonverzuim; Veelverzuim.	4 november 2020
OB Bijzondere normen	9 november
DAS tool	12 november



© 2020 KPMG Advisory N.V., ingeschreven bij het handelsregister in Nederland onder nummer 33263682, is lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Cooperative (“KPMG International”), een Zwitserse entiteit. Alle rechten voorbehouden. De naam KPMG en het logo zijn geregistreerde merken van KPMG International.

Appendix B – Bestudeerde documentatie



Wij hebben onderstaande documenten bestudeerd.

Naam product	Documentnaam
Brancheinformatie	Branchcijfers WIA WMK 1.3
	Bracheinfo LH WMK 1.2
	Bracheinfo OB WMK 1.3
DAS-tool	Presentatie OSVO aangiftesystematiek
	Codetabel response message LH 2020 v1.0 24 April 2019
	Rekenvoorschriften voor geautomatiseerde loonadministratie LH
	Beschrijving Velden per jaar 2020
	Gegevensspecificaties aangifte loonheffingen 2021 v2.0 09-07-2020
	Toelichting loonberekening voor lh
	LOA XXL – kwaliteit LAB en LH-keten
	Handreiking DAS applicatie met ophaalfunctie 2020 v1.2
	Evaluatieformulier PIA LH-DAS
	PIA Rijksdienst LH Analyse
	Risicoanalyse DAS-server
	Nota privacy Risico's DAS Server
	Gruff Logging
	2019-05-20 Voorwaarden gebruik Gruff
	Gruff autorisaties
Gruff	Evaluatieformulier PIA Gruff
	Nota privacy Risico's Gruff
	WMK-toets EHI Relatievisualisatie v.1.0

Naam product	Documentnaam
Intranetportal Service 4u	Risicoanalyse OSINT producten
	Risico's en maatregelen OSINT Marktplaats
Marktplaats	Marktplaats data
	Nota privacy Risico's OSINT Marktplaats
	Werkwijze Marktplaats vordering
	WMK-toets EHI OSINT product Marktplaats v1.0
SIDN	Sidn voorbeeld bd
	Werkwijze SIDN aanvraag
	Nota privacy Risico's SIDN
	SIDN data
	WMK-toets EHI OSINT product SIDN



© 2020 KPMG Advisory N.V., ingeschreven bij het handelsregister in Nederland onder nummer 33263682, is lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Cooperative ("KPMG International"), een Zwitserse entiteit. Alle rechten voorbehouden. De naam KPMG en het logo zijn geregistreerde merken van KPMG International.



Contacten

De contactpersonen van KPMG voor dit rapport zijn:

[Redacted]

[Redacted] Assurance & Advisory

Tel: 06 - [Redacted]

Email: [Redacted]@kpmg.nl

[Redacted]

[Redacted] Data Privacy

Tel: 06 - [Redacted]

Email: [Redacted]@kpmg.nl

