Belastingdienst

MT DF&A

Corporate Dienst
Datafundamenten & Analytics

Croeselaan14
3521 CA Utrecht
www.belastingdienst.nl

Contactpersoon

[redacted]@belastingdienst.nl

memo

Definitief: Reactie DF&A op KMPG onderzoek oud EH&I-producten

Datum
9 maart 2021

2

Bijlage:
A2000021206 RA KPMG-rapport AVG-onderzoek Belastingdienst DFA-EHI def 20210125

Aanleiding
DF&A heeft aan KPMG gevraagd een onderzoek uit te voeren naar oud EH&I-producten en deze te toetsen aan compliantie met de AVG, interne standaarden & richtlijnen en de Gouden Regels van DF&A.
KPMG heeft dit onderzoek uitgevoerd en vastgelegd in het "Onderzoek naar oud-EH&I-producten bij DF&A; Definitief onderzoeksrapport inzake naleving van AVG, Archiefwet, QA-standaarden en Gouden Regels d.d. 25 januari 2021, hierna: het "Onderzoeksrapport".
In deze memo wordt de reactie vanuit het MT van DF&A verwoord met de bedoeling deze aan het Onderzoeksrapport aan te hechten. Het Onderzoeksrapport dient derhalve altijd in combinatie met deze reactie te worden gelezen.

Algemene reactie MT DF&A
Het Onderzoeksrapport geeft per peildatum 1-9-2020 een beeld van de producten en diensten die DF&A levert vanuit het oude EH&I portfolio. Producten en diensten vanuit het oude EH&I portfolio die per die datum bij DF&A niet meer in productie staan/niet meer worden geleverd zijn niet in het onderzoek meegenomen.

DF&A is blij met deze externe toets. Het geeft overzicht en inzicht. DF&A gebruikt dit onderzoek om deze producten en diensten hun plek te geven binnen DF&A en binnen de Belastingdienst als geheel, met aandacht voor de observaties en aanbevelingen uit het Onderzoekrapport.

DF&A beziet het onderzoek en de resultaten hieruit binnen de volgende context:

1. *Verantwoordelijk DF&A versus verantwoordelijkheid andere dienstonderdelen binnen de Belastingdienst*

De scope van het onderzoek is begrensd tot DF&A.
KPMG heeft voor dit Onderzoeksrapport de opdracht gekregen om *binnen* DF&A medewerkers te interviewen en documenten te bestuderen. In een aantal gevallen is de documentatie niet opgeleverd omdat die bij het verantwoordelijke dienstonderdeel (als opdrachtgever/gebruiker/afnemer) hoort. Binnen DF&A is derhalve niet bekend of bepaalde documenten bestaan of dat de benodigde informatie anderszins is vastgelegd door de betreffende dienstonderdelen.

Daarom behoeft een aantal zaken uit het Onderzoeksrapport overleg met die dienstonderdelen om te zorgen dat ook vanuit de opdrachtgevers/afnemers/gebruikers van de producten/diensten wordt gezorgd voor het voldoen aan geldende wet- en regelgeving.

2. *Momentopname*

Het onderzoek door KPMG is een momentopname, uitgevoerd in oktober – november 2020.
DF&A is voortdurend bezig om de kwaliteit van haar producten en diensten te borgen en te verbeteren. Dat is uiteraard ook na de interviews en documentstudie door KMPG door DF&A gecontinueerd. Ook heeft dit onderzoek zelf geholpen om aandacht te krijgen voor een aantal zaken die voorheen onderbelicht waren. Een aantal observaties/aanbevelingen van KPMG in het Onderzoeksrapport is reeds opgevolgd door DF&A. Met name door het project "DF&A geborgd" zijn acties uitgevoerd rondom dataretentie/ bewaartermijnen. Met als resultaat dat op 31-12-2020 de producten uit het Onderzoeksrapport die op het exploitatie overzicht van DF&A staan, voldoen aan de bewaartermijnen.

Aanbevelingen/conclusies

[redacted] het MT gehoord hebbende, besluit dat:

1. Het Onderzoeksrapport wordt vastgesteld door het MT. Met daarbij de complimenten aan iedereen die hieraan heeft meegewerkt.
2. De producten uit het Onderzoeksrapport worden, waar dit nog niet het geval is, opgenomen in het portfolio en de voortbrengings- en exploitatieprocessen van DF&A.
3. Onderzocht wordt hoe advieswerk opgenomen kan worden in het portfolio en de voortbrengings- en exploitatieprocessen van DF&A.
4. De uitkomsten van het onderzoek worden gecommuniceerd met de afnemers, te beginnen bij de afnemers van producten met hoog risico volgens het rapport.
5. Er duidelijkheid moet worden verkregen over de door KPMG geformuleerde non-compliantie in de bewaartermijnen van de producten uit het Onderzoeksrapport.

Communicatie

Het Onderzoeksrapport en het MT besluit zullen worden gecommuniceerd aan de medewerkers van DF&A.
[redacted] zal de betrokken directeuren informeren en het Onderzoeksrapport zal geagendeerd worden voor driehoeksoverleg FJZ/UHB en IV&D.

Scope afbakening

Het onderzoek en het Onderzoeksrapport richt zich op de producten en diensten met als peildatum 1-9-2020.

Er zijn door de Tweede Kamer vragen gesteld over de EH&I periode 2012-2018. Dit zal worden opgepakt binnen HVB (Herstellen, Verbeteren, Borgen).

In de periode na EH&I (2018-2020) zijn producten bij DF&A opgenomen. Met UHB en IV&D zal besproken worden of en hoe hier nader onderzoek moet plaatsvinden naar de producten en diensten die in deze periode zijn geleverd.

Onderzoek naar oud-EH&I-producten bij DF&A

Definitief onderzoeksrapport inzake naleving van AVG, Archiefwet, QA-standaarden en Gouden Regels

25 januari 2021

A2000021206 RA

KPMG Advisory NV
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Tel: +31 (0)20 656 7890
Fax: +31 (0)20 656 8125

Belastingdienst
DF&A
[redacted]
Croeselaan 14
3521 CA UTRECHT

Amstelveen, 25 januari 2021

Geachte [redacted]

Namens KPMG Advisory N.V. (hierna: KPMG) danken wij u hartelijk voor de mogelijkheid die u ons hebt gegeven om een onderzoek inzake de oud-EH&I-producten uit te mogen voeren bij de Belastingdienst. In dit rapport presenteren wij de resultaten van het onderzoek. Wij hebben dit onderzoek uitgevoerd conform ons "Voorstel voor onderzoek naar oud-EH&I-producten bij DF&A", d.d. 1 oktober jl. (met uw referentie UIC20-71 en ons kenmerk A2000021206 VO).

Het doel van het onderzoek is het inzicht verschaffen in welke mate de in scope geplaatste oud-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. Deze analyse is uitgevoerd door het voeren van diverse gesprekken met medewerkers van de Belastingdienst en het bestuderen van de beschikbaar gestelde documentatie.

Uw reacties op de twee afgestemde conceptversies (d.d. 20 november en 4 december jl.) hebben wij in deze finale versie verwerkt. Naar aanleiding van de bespreking in uw MT-overleg 13 januari jl. hebben wij de tekst geactualiseerd met uw analyse van bewaartermijnen en met verduidelijking van scope en DF&A-rol aangebracht.

Deze rapportage vormt de afsluiting van onze overeengekomen werkzaamheden. Wij hebben de plezierige samenwerking met uw organisatie tijdens dit intensieve traject zeer op prijs gesteld en hopen onze relatie met uw organisatie te mogen continueren.

Mochten er nog vragen zijn met betrekking tot dit rapport, schroom dan niet om contact met [redacted] of mij op te nemen (de contact-gegevens zijn op de laatste pagina van dit rapport opgenomen).

Hoogachtend,
KPMG Advisory N.V.

[redacted]

© 2021 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

Inhoudsopgave

1. Achtergrond, doel, scope en aanpak **4**

2. Managementsamenvatting **8**

3. Detailoverzicht

Categorie 1 **12**

Categorie 2 **16**

Categorie 3 **15**

Bijlagen **35**

A – Lijst van interviews

B – Bestudeerde documentatie

C – Lijst van oud-EH&I-producten

© 2021 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 (1/3)

Aanleiding

Om de taken van de Belastingdienst sneller en gerichter uit te voeren, combineert DF&A (persoons)gegevens uit verschillende systemen om deze vervolgens op te werken naar datafundamenten, waaruit vervolgens weer analyseproducten worden gemaakt. Het werken met deze (persoons)gegevens hangt nauw samen met de bescherming van de 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. Recentelijk zijn oud-EH&I-producten toegevoegd aan het DF&A-portfolio. Mogelijk zijn niet al deze oud-producten tijdens de totstandkoming onderworpen aan het huidige proces van Standaarden en Richtlijnen van DF&A.

Doel

Binnen DF&A bestaat daarom de wens om een onderzoek te laten uitvoeren naar de 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 kader dat wij hebben gehanteerd in onze rapportage 'Verwerking risicoselectiesignalen voor toezicht' d.d. 10 juli 2020.

Scope en aanpak

Om binnen de beoogde tijdlijnen gedegen antwoord te kunnen geven op uw onderzoeksvraag, hebben wij een gefaseerde aanpak gehanteerd die ons in staat stelde om in kort tijdbestek tot de kern te komen.

Een uitgebreide beschrijving van onze gelaagde aanpak volgt in het volgende hoofdstuk, 'Ons plan van aanpak'.

Met betrekking tot de scope, betekent dit het volgende:

- Wij hebben de door u gemaakte selectie van de 50 EH&I-producten, deze allen onderworpen aan een analyse met een gelijkwaardige mate van diepgang. Over de EH&I-producten die een laag privacy risicoprofiel vertoonden is minder uitvoerig gerapporteerd, aangezien de meeste normen en standaarden daarop 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 hebben gericht op de mate waarin deze producten voldoen aan de basisbeginselen van de AVG.
- Ons onderzoek omvatte niet het uitvoeren van Gegevensbeschermingeffect-beoordelingen (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 de ter beschikking gestelde documentatie en gehouden interviews, wij hebben geen zelfstandige analyse van de verwerkingen, hiervoor gebruikte systemen en AVG-naleving uitgevoerd.
- Gedurende de inventarisatie hebben wij voornamelijk gekeken naar de producten, diensten en activiteiten van DF&A. Deze activiteiten vinden plaats in een bredere context en in samenwerking met, of geheel ten behoeve van, andere dienstonderdelen. De eindverantwoordelijkheid voor die verwerkings-activiteiten ligt veelal bij de primaire processen en derhalve buiten de DF&A-keten. De (primaire) verwerkingsprocessen en bijbehorende documentatie van die dienstonderelen vielen buiten de scope van deze inventarisatie.
- In de detailbevindingen benoemen wij categorieën van persoonsgegevens die worden verwerkt in het product. Deze opsomming kan niet worden beschouwd als een limitatieve lijst van verwerkte persoonsgegevens.

KPMG © 2021 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 (2/3)

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. Dit is besproken in het interview waar de andere FIOD-producten besproken zijn, en vervolgens afgestemd met opdrachtgever.

— Poort IH is niet meegenomen in onze analyse omdat dit product geen verbinding met DF&A heeft. Het betreft hier enkel een vanuit DF&A gedetacheerd persoon.

— Met betrekking tot producten/diensten ten 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.

Definities

Zoals in de aanpak op de vorige pagina beschreven zijn de producten tijdens het onderzoek in drie verschillende categorieën ingedeeld. Hieronder zijn de volgende drie 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 van 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. Dit risiconiveau wordt tevens uitgelicht in de management samenvatting.

+	Voldoet, is in voldoende mate aangetoond op basis van documentatie en aanvullende toelichting vanuit interviews.
+/-	Voldoet gedeeltelijk, er wordt gedeeltelijk voldaan aan de gestelde eisen, maar dit kan niet volledig aantoonbaar worden gemaakt vanuit documentatie, of de gestelde maatregelen zijn niet volledig genoeg om alle risico's tot een acceptabel niveau terug te brengen.
-	Voldoet niet aan de norm en/of dit kan leiden tot een (hoog) risico, documentatie ontbreekt of is niet aan ons beschikbaar gesteld.

Methodische Aanpak

De managementsamenvatting bevat een tabel met alle producten uit categorieën 2 en 3 en de mate waarin deze voldoen aan de 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

iii. voldoet gedeeltelijk en als volgt gedefinieerd:

Deze evaluatie is gebaseerd op de detailbevinden waarin de kernvereisten nader worden toegelicht en de risico's worden geïdentificeerd. Op basis van de detailbevindingen hebben wij een algeheel risicoclassificatie per product of dienst bepaald. Deze risicoclassificatie geeft inzicht in hoeverre wordt voldaan aan de AVG, Archiefwet en andere normen en hoe wij de risico van een serieuze inbreuk op één van deze normen inschatten.

© 2021 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 (3/3)

Risicoclassificatie

Nu de analyse die is uitgevoerd heeft plaatsgevonden in een relatief kort tijdsbestek en met een beperkte scope, kunnen wij geen uitvoerig oordeel opstellen of de producten en diensten in scope wel of niet voldoen aan alle aspecten van de AVG, Archiefwet, QA-standaarden en Gouden Regels. Wel hebben wij kunnen constateren in welke mate de in scope producten of diensten risico's lopen op (serieuze) inbreuken op de bovengenoemde kaders. Wij classificeren daarbij:

- **L** Laag risico: wij hebben niet geconstateerd dat de gegevensverwerking inbreuk maakt op de basisprincipes van de AVG. De maatregelen voor het zorgvuldig en veilig verwerken van de gegevens zijn goed op orde of behoeven slechts minimale tot geen verbetering.
- **M** Midden risico: wij hebben niet geconstateerd dat de gegevensverwerking inbreuk maakt op de basisprincipes van de AVG. De maatregelen voor het zorgvuldig en veilig verwerken van gegevens behoeven op bepaalde punten verbetering.
- **H** Hoog risico: de Belastingdienst heeft niet of onvoldoende met documentatie kunnen aantonen dat het betreffende product toereikend voldoet aan de basisprincipes van de AVG. De maatregelen voor het zorgvuldig en veilig verwerken van de gegevens behoeven op korte termijn verbetering.

Zoals is af te lezen in de classificaties maken wij onderscheid in twee bepalende factoren:

- Is er inbreuk op een basisprincipe van de AVG (of Gouden Regels) waargenomen? Voorbeelden van inbreuken op fundamentele principes zijn het ontbreken of niet kunnen onderbouwen van een rechtmatige grondslag, het verwerken van persoonsgegevens buiten de oorspronkelijke doelbinding, de verwerkingsactiviteit is niet proportioneel aan het gestelde verwerkingsdoel, etc. M.a.w. persoonsgegevens hadden dan niet zo verwerkt mogen worden.
- Naast het feit of de gegevens wel of niet verwerkt hadden mogen worden, kijken wij naar de waarborgen en maatregelen rondom de verwerking van persoonsgegevens. Daarmee kijken wij of de gegevens wel veilig worden opgeslagen, of deze zorgvuldig worden verwerkt en met voldoende waarborgen omkleed dat dit ook zo blijft.

Leeswijzer

Hierna volgt eerst een managementsamenvatting met een overzicht van de mate waarop de producten voldoen aan een aantal met de opdrachtgever afgestemde geselecteerde kernvereisten uit de AVG, de Archiefwet en uw Quality Assurance (QA) kaders, inclusief de door DF&A intern gehanteerde Gouden Regels.

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.

KPMG © 2021 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

2. Management-samenvatting

2. Managementsamenvatting (1/3)

Aanleiding en onderzoeksvraag

Om de taken van de Belastingdienst sneller en gerichter uit te voeren, combineert DF&A (persoons)gegevens uit verschillende systemen en bronnen. 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 jl. De aanpak is in detail beschreven in de offerte d.d. 1 oktober jl. 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 (indien noodzakelijk) aanvullende toetsingen, zoals een QC-toets, AVG-scan of GEB. Met betrekking tot de oud-producten van EH&I is gebleken dat een aantal van de te onderzoeken producten en/of diensten niet onderworpen zijn aan dergelijke toetsingen of dat deze niet meer vindbaar zijn. Als gevolg konden voor deze rapportage slechts voor een beperkt aantal producten dergelijke toetsingen worden geanalyseerd.

Verantwoordelijkheid
Vanuit de gesprekken en documentatie hebben wij niet altijd kunnen vaststellen wie de eigenaar van de gegevens is, zodra deze wordt gedeeld buiten DF&A. Een aantal producten en/of diensten omvat 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 of inconsistent worden nageleefd of als dat wel gebeurt, dit niet aantoonbaar is.

Van belang is om hierbij te vermelden dat een DF&A-product kan zijn ingezet in één of meer primaire verwerkingsprocessen, waardoor de eindverantwoordelijkheid voor denaleving van wet- en regelgeving (b.v. AVG en Archiewet) en vereiste activiteiten (b.v. GEB) ligt bij het lijnmanagement van het betreffende dienstonderdeel. DF&A vervult in een dergelijke situatie een gespecialiseerde, faciliterende rol, waarbij ze kan zorgdragen voor de naleving van het DF&A-deel van de gehele keten. Die verdere verwerking van deze gegevens buiten DF&A is daarmee ook buiten scope van dit onderzoek gebleven.

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:

- *FIOD Berlijn – Trailer;*
- *FIOD Centraal punt BTW-fraude;*
- *Team aanpak risicovolle netwerken.*

Deze producten hebben allen 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. Daarmee zijn niet alle wettelijke waarborgen in voldoende mate ingericht en ontstaan er risico's omtrent het niet rechtmatig verwerken van (gevoelige) persoonsgegevens.

Indien een product of dienst wordt geclassificeerd met een hoog risico, dan adviseren wij de Belastingdienst deze gegevensverwerking nader in detail op compliance met AVG en Archiefwet te onderzoeken. Een GEB zou hiervoor een adequaat instrument kunnen zijn, gevolgd door het oplossen van daarin geïdentificeerde privacyrisico's. Bij producten of diensten met een midden risico kan met aanvullende documentatie en nader te treffen maatregelen de gegevensverwerking beter worden geborgd opdat kan toereikend worden voldaan aan externe en interne vereisten.

© 2021 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

2. Managementsamenvatting (2/3)

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	Rechtmatige grondslag	Doelbinding	Proportionaliteit	Opslag van gegevens	Gegevensuitwisseling (intern en extern)	Data-retentie	Toegangsrechten	Risico-Indicatie
Op basis van welke normen	*AVG, QA/QC*	*AVG*	*AVG, QAQC, Gouden Regel nr. 5*	*AVG, QAQC, Gouden Regel nr. 6*	*AVG, Gouden Regel nr. 2*	*AVG, Gouden Regel nr. 3*	*AVG, Archiefwet*	*AVG, Gouden Regel nr. 7*	*Algeheel*
Schoonmaakbranche	-	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	L
Schijnconstructies	-	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	L
Uitzendbranche	-	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	L
OB telefoonverzuim	+	+	+	+/-	+	+	-	+	L
OB tweeverzuim/ Veelverzuim	+	+	+	+/-	+	+	-	+	L
Bijzondere normen	+	+	+	+	+	+	-	+	L
Branche-informatie	+	+	+	+	+	+	+/-	+	L
FIOD Bijzondere Taken	-	+/-	+/-	+/-	+	+	+/-	+	M
SIDN	+	+	+	+	+	+	-	+	L

H Hoog risico

M Midden risico

L Laag risico

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

KPMG © 2021 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

2. Managementsamenvatting (3/3)

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

Naam & inherent privacyrisico	Documentatie	Rechtmatige grondslag	Doelbinding	Proportionaliteit	Opslag van gegevens	Gegevensuitwisseling (intern en extern)	Data retentie	Toegangsrechten	Risico-Indicatie
Op basis van welke normen	*AVG, QA/QC*	*AVG*	*AVG, QAQC, Gouden Regel nr. 5*	*AVG, QAQC, Gouden Regel nr. 6*	*AVG, Gouden Regel nr. 2*	*AVG, Gouden Regel nr. 3*	*AVG, Archiefwet*	*AVG, Gouden Regel nr. 7*	*Algeheel*
Marktplaatsverzoek	+	+	+	-	+	+	-	+	L
DAS-tool	+	+/-	+/-	+/-	+/-	+	+/-	+/-	M
Zeer vermogende personen	+	+	+	+	+	+	+	-	M
Gruff Netwerk-analysetool	+	+	+	-	+	+	+/-	+/-	M
FIOD Berlijn – Trailer	-	+	+/-	+/-	+	+	-	+	H
FIOD Centraalpunt BTW-fraude	-	+	+/-	+/-	+	+	-	+	H
FIOD – AMLC*	-	+	+/-	+/-	+	+	-	+	M
Team aanpak risicovolle netwerken	-	+/-	+	+	+	+	-	+	H
Signaalanalyse postbus	+	+/-	+/-	+/-	+	+	+	+	M

H Hoog risico M Midden risico L Laag risico

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

* FIOD AMLC scoort een algeheel lager risico dan bijvoorbeeld FIOD Centraalpunt BTW-fraude of Berlijn – Trailer – ondanks dezelfde individuele scores – omdat het inherente risico (naar gelang de aard en omvang van de persoonsgegevens) van deze dienstverlening lager is.

KPMG © 2021 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

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
DG 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

© 2021 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

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
Landelijk coördinator EOS	Niet aanwezig	Dit betreft een rol. Als er nieuwe fraudefenomenen opduiken, wordt in deze rol kennis tussen afdelingen uitgewisseld. Dat gebeurt op fenomeenniveau; hierbij worden geen persoonsgegevens verwerkt.
Fraudecoördinator	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 persoons-gegevens. Als dit het geval is, dan loopt dit tegenwoordig via het stramien 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 fraudeteams 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, risicoscenario's en andere indicatoren, maar geen individuele gevallen en dus geen persoonsgegevens.
Werkgroep faillissementsfraude (Min. JenV)	Niet aanwezig	Dit betreft kennisdeling met meerdere ministeries en onder leiding van het Min van J&V, 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	DFEX-149	Dit betreft de intranetsite die draait op de infrastructuur van de Belastingdienst.

© 2021 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

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 voortkomt, 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 IFFC 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 aan het notariaat. Het doel is het preventief adviseren om het fraudebewustzijn te verhogen, zodat ze aan de voorkant fraude kunnen tegengaan. Daarnaast is er ook twee keer per jaar een overleg over fenomenen en hoe hiermee om te gaan.

© 2021 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

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

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

	Schoonmaakbranche DFEX-171 Schijnconstructie DFEX-170				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Schoonmaakbranche	Deze activiteit betreft een incidentele informatieaanvraag inzake 'risicovolle' bedrijven in de schoonmaakbranche. Dit betreft een extern verzoek. De gegevens-uitwisseling berust op een convenant met partners, zijnde (o.a.) ministerie(s). De gegevens worden 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, aangezien nog geïnventariseerd wordt hoe de oplevering zal plaatsvinden. Deze zal voorafgaand aan oplevering worden onderworpen aan het huidige proces van standaarden en richtlijnen van DF&A, waaronder ook de WMK-toets. De gegevens worden vervaardigd met een query uit te oefenen op een data-fundament, waarna deze wordt vormgegeven in een Excel-bestand. Bij gegevens-uitwisseling vanuit DF&A/MKB naar de externe partner is het Excel-bestand beveiligd met een wachtwoord. *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 QA-kaders, inclusief de door DF&A intern gehanteerde Gouden Regels.*	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'.	*Gegevensuitlevering heeft vooralsnog niet plaats-gevonden dit jaar. Er zijn daarom geen risico's gedefinieerd.*		L
Schijnconstructies*	*incl. LSI: Fenomenen, risicodetectie subject, Grensoverschrijdend werk Deze activiteit betreft een incidentele informatieaanvraag inzake 'risicovolle' bedrijven. Dit betreft een extern verzoek. De gegevensuitwisseling berust op een convenant met de partners, zijnde ministerie(s). De gegevens worden 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. *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 QA-kaders / Gouden Regels.*	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'.	*Gegevensuitlevering heeft vooralsnog niet plaats-gevonden dit jaar. Er zijn daarom geen risico's gedefinieerd.*		L

KPMG © 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	Uitzendbranche, DFEX-163				
	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 volgens de lijnen van handhavingsregie rechtspersonen in de uitzendbranche aan te leveren die voldoen aan 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 WMK-toets worden uitgevoerd en zullen voorwaarden worden opgesteld over hoe en welke gegevens worden aangeleverd. *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 managementsamenvatting en dus de AVG, de Archiefwet en uw QA-kaders / Gouden Regels.*	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'.	*Gegevensuitlevering heeft vooralsnog niet plaatsgevonden dit jaar. Er zijn daarom geen risico's gedefinieerd.*		L

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	OB TELEFOONVERZUIM, DFEX-148				
	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 bellijst. Medewerkers van KI&S (klantinteractie) nemen contact op met de ondernemers om hen te wijzen op hun deadline. Het wordt gezien als serviceverlening. Er is momenteel geen feedbackloop 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 heffen en innen van belastingen en het uitkeren van toeslagen. **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.	MM GEB	L

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	OB Tweeverzuim/Veelverzuim, DFEX-19				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
OB Tweeverzuim/Veelverzuim	**Algemeen kenmerken gegevensverwerking** *Gelijk als OB Telefoonverzuim.* 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 bellijst vanuit DF&A verkregen. **Rechtmatige Grondslag:** Valt onder de wettelijke taak van de Belastingdienst, het heffen en innen van belastingen en het uitkeren van toeslagen. **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 aangiftegegevens 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:** Historie wordt bewaard om te kunnen voldoen aan vervolgklantvragen. Er zijn echter geen termijnen afgestemd hoe lang deze gegevens beschikbaar blijven. • 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.	MM GEB	L

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	OB Bijzondere Normen, DFEX-155				
	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 gegevenskwaliteit 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 gegevenskwaliteit te borgen. De query-output wordt vervolgens in een Excel-bestand aangeleverd bij de manager van MKB. Dit gebeurt via 'ConnectPeople, waarvan alleen een afdelings-manager 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 wordt na overdracht aan MKB bewaard. **Rechtmatige Grondslag:** Valt onder de wettelijke taak van de Belastingdienst, het heffen en innen van belastingen en het uitkeren van toeslagen. **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 gegevenskwaliteit. 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. Op basis van documentatie kan worden vastgesteld dat de output niet met minder brongegevens vervaardigd kan worden en daarmee in lijn is met de proportionaliteit- en subsidiariteits-beginselen.	• Er is geen bewaartermijn vastgesteld voor het bewaren van de Excel-lijst. Deze worden ook niet verwijderd. • **Dataretentie:** Historie wordt bewaard om te kunnen voldoen aan vervolgklantvragen. Er zijn echter geen termijnen afgestemd hoe lang deze gegevens beschikbaar blijven.	MM WMK GEB	L

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	Branche informatie (Loondienst) DFEX-150 Branche informatie (WIA en omzetbelasting) DFEX-152				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Branche-informatie	**Algemeen kenmerken gegevensverwerking** *Branche-informatie Loondienst/WIA en omzetbelasting* Op de intranet pagina voor interne inspecteurs van de Belastingdienst is een informatiepagina waar onder het kopje 'Branche-informatie' de aangiftes 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-aangiftes uiteengezet zodat inspecteurs kunnen benchmarken met landelijke gemiddeldes. De informatie wordt per branchecode weergegeven op geaggregeerd niveau. Het doel is om de OB-aangiftes 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. Gegevens worden onttrokken uit één datafundament en vervaardigd door het medewerkers van het daarvoor aangewezen 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 toezicht-houden. **Gegevensuitwisseling derden:** Er worden geen gegevens gedeeld met derden. **Dataretentie:** Wij hebben vernomen dat alle bronbestanden en tussenresultaten binnen de gestelde termijnen van de archiefwet (na zeven jaar) worden verwijderd. Wij hebben dit niet kunnen vaststellen in documentatie of richtlijnen.	De betrokkenen zijn ondernemers. Persoonsgegevens worden geaggre-geerd in het overzicht, dus zijn op basis van de overzichten niet herleidbaar tot individu. De ruwe data bestaan 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 disproportioneel is ten opzichte van het gestelde verwerkingsdoel.	• Wij hebben vernomen dat alle bronbestanden en tussenresultaten binnen de gestelde termijnen van de Archiefwet worden verwijderd. Wij hebben dit niet zelf in documentatie of richtlijnen kunnen vaststellen. Mogelijk zijn dergelijke termijnen niet geformaliseerd.	WMK	L

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	FIOD Bijzondere Taken, geen DFEX –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 gegevensoverdracht, maar het komt voor dat kennis gedeeld wordt op individueel niveau om kennis, zicht en samenhang tussen verschillende subjecten in kaart te brengen. 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. **Rechtmatige Grondslag:** Valt onder de wettelijke taak van de Belastingdienst van fraude opsporen en toezichthouden. **Doelbinding:** Het doel is in lijn met het doel innen van belastingen en toezichthouden hierop middels opsporing. **Gegevensuitwisseling derden:** Er worden geen gegevens gedeeld met derden.	Voor het onderzoek dat DF&A uitvoert worden gewone en vertrouwelijke persoonsgegevens verwerkt die uit de bronsystemen komen. Hierbij worden geen bijzondere persoonsgegevens, bijvoorbeeld ten aanzien van etniciteit, verwerkt. **Proportionaliteit:** Gezien de aard van de verstrekte persoonsgegevens (NAW-gegevens) is de gegevensverwerking proportioneel.	• **Dataretentie:** Het is onduidelijk hoelang de persoonsgegevens worden bewaard. Hierbij wordt opgemerkt dat dit de verantwoordelijkheid van FIOD is, en niet die van DF&A. Het is mogelijk dat de FIOD daarvoor adequate processen heeft ingeregeld. Het analyseren daarvan valt buiten de scope van deze analyse. • Er worden slechts incidenteel persoonsgegevens ingezien door DF&A, maar niet verder opgeslagen op systemen van DF&A. • Doordat er geen vastlegging (in de vorm van een GEB, WMK of anderszins) is, kan ook geen verantwoording achteraf plaatsvinden. • Door bovenstaande risico's, in verhouding tot de gevoelige context waarin ze verwerkt worden, schatten wij het algehele risico in op 'midden'.		M

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	SIDN DFEX-153				
	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 het daarvoor aangewezen team binnen 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, toezichthouden. **Doelbinding:** Het doel is in lijn met het doel innen van belastingen en toezicht-houden. **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 contact-informatie van de natuurlijke persoon die de domeinnaam bij SIDN heeft geregi-streerd. Het gaat hierbij om telefoon-nummer, 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 gegevens in het SIDN-register niet altijd de actuele situatie rondom een persoon weergeven maar de situatie zoals laatst is doorgegeven via de registrar van het domein. Dit is inherent aan de opzet van het register. Onjuiste interpretatie van de gegevens in het register kan het risico geven dat onjuiste persoonsgegevens worden verwerkt. • De SIDN-gegevens wordt buiten DF&A bewaard, namelijk bij de uiteindelijke eindgebruiker van de ontvangen gegevens. Het is onduidelijk hoelang de betreffende persoonsgegevens worden bewaard. DF&A heeft met een disclaimer aange-geven dat de eindgebruiker hier zelf adequate maatregelen voor dient te treffen, voordat zij gebruikmaken van deze dienst.	WMK MM	L

© 2021 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

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
M Risiconiveau Midden
L Risiconiveau Laag
MM Memo privacyrisico's
WMK WMK
GEB GEB/AVG-scan

	DAS-tool, DFEX-179				
	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 loonaangifteketen om de oorzaak van fouten op te kunnen sporen. Hierbij maakt de DAS-tool gebruik van de XML-berichten die in het Digitaal archiefsysteem (DAS) worden opgeslagen. De bron van de gegevens is de werkgever zelf, via de loonaangiftes. De DAS-tool wordt voor twee doeleinden gebruikt: • Technische analyse door Analyseteam Gegevenskwaliteit (AGL), een samenwerking tussen de Belastingdienst (BD) en UWV, waarbij maandelijks de stand van het collectieve deel van de aangiftes (BD) wordt vergeleken met het nominatieve totaal van de aangiftes (UWV). Geconstateerde verschillen worden geanalyseerd en behandeld. • Inhoudelijke analyse door medewerkers controle en administratie (zie: "Handreiking Das_applicatie met ophaalfunctie 2020 V1.2.pdf"). De DAS-tool is in staat om tijdsbeelden te vormen en daardoor het historisch verloop van de aangiftes loonheffingen te tonen. De tool kan objectieve regels toetsen b.v. of een sofi-nummer aan de 11 proef voldoet. De tool werkt separaat van andere systemen/applicaties. **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 (SAP Business Objects) naar het UWV waardoor de polisregistratie van een werkgever te benaderen is en kan worden vergeleken. Alleen AGL-analisten hebben toegang tot de poort. **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 UWV, die bepalend in wat niet opgenomen mag worden in een uitdraai/export. Deze kruisjeslijst is de lijst met gegevens waarvan het UWV 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 polisadministratie. Periodiek wordt een beeld opgevraagd van een polis en de daarmee samenhangende technische sleutels. Een dergelijke technische sleutel (hashkey/totaal-key) is een samenvoegsel van onder meer het BSN, LH-nummer, numerieke inkomstenverhouding (IKV) en aangifteperiode. Bij ontbreken van het BSN wordt daarvoor in de plaats het personeelsnummer opgenomen in de sleutel. Verder worden de hoogte van loon en premie(korting) 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 het volgende risico: • Een risico dat in de GEB wordt omschreven is die van doelbinding. Dit speelt wanneer de gearchiveerde persoonsgegevens verder worden verwerkt, zoals bijvoorbeeld voor inzage en/of analyse, die niet langer verenigbaar zijn met het oorspronkelijke verwerkingsdoel.	GEB MM	M

KPMG © 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	Zeer vermogende personen, DFEX-159				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Zeer vermogende personen	**Algemeen kenmerken gegevensverwerking** Het programma zeer vermogende personen (ZVP) past individuele klantbehandeling toe aan de meest vermogende particulieren, onder andere vanwege de complexiteit van zaken. Het is daarom van belang inzicht te hebben in de populatie en vermogenspositie van deze personen. Vanuit DF&A wordt een lijst van de circa 1.500 meest vermogende personen vervaardigd. Enerzijds heeft het programma het doel om individuele klantbehandelaars toe te kennen aan de zaken, anderzijds heeft het programma een signaalfunctie op het gebied van erf- en schenkrecht. De gegevens worden 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 krijgen vervolgens aan de hand van deze lijst klanten toebedeeld. De frequentie van het opstellen en aanleveren van deze informatie is vier keer per jaar. Het overzicht wordt samengesteld op (een kopie van) een database via SQL-query's en SAS-scripts. Deze query's wordt 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 manager van GO. Dit gebeurt via 'Connect-People', waarvan alleen één GO-manager en één DF&A-medewerker het wachtwoord en daarmee toegang hebben. **Rechtmatige grondslag:** De rechtmatige grondslag is vastgelegd in de WMK, een taak van algemeen belang. **Doelbinding:** Valt onder de wettelijke taak van de Belastingdienst, het heffen en innen van belastingen en het uitkeren van toeslagen. **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 o.a.: BSN, financiële informatie zoals saldi lopende rekeningen, saldi spaarrekeningen, schulden, giften, schenkingen, geldstromen binnen de BV, informatie omtrent vermogen (vastgoedobjecten en BV's, fiscaal partnerschap, informatie omtrent de samenstelling van het huishouden. **Proportionaliteit:** De output is een beperkte lijst met personen en kan niet op een andere wijze worden samengesteld. De benodigde informatie inclusief verantwoording is gedocumenteerd en aan ons beschikbaar gesteld. Daarnaast is de proportionaliteit getoetst en akkoord bevonden in een WMK-toets.	• De query-code van de zoekopdracht(en), de opzichzelfstaande query en script(s) zijn niet conform eerdere genoemde beginselen (en op basis van het 'need-to-know'-beginsel) afgeschermd. De code staat namelijk in een gebied waar alle oud EHI medewerkers toegang toe hebben. Dit leidt mogelijk tot het risico dat te veel personen inzage kunnen verkrijgen in deze gegevens, wanneer deze ook toegang hebben tot de achterliggende database. Uit interviews blijkt dat de Belastingdienst voornemens is eind dit jaar de code over te zetten tot een gebied met beperkte toegang. Als gevolg zal dit risico vervallen en het hierbij vastgestelde risico-classificering ook. • Ondanks dat er een uitgebreide WMK en een privacymemo is opgesteld, adviseren wij om alsnog een volledige GEB op te stellen om alle privacyrisico's volledig mee in kaart te brengen. Dit bevelen wij voornamelijk aan gezien de gevoeligheid van de gegevens die worden verwerkt. Op basis van de bevinding inzake de query-code en het ontbreken van een formele GEB in combinatie met de hoge mate van gevoeligheid van de gegevens, kwalificeren wij dit als een midden risico.	WMK MM	M

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

Gruff Netwerkanalysetool DFEX-17					
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Gruff Netwerkanalysetool	**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 Belastingdienstkunnen hiervan gebruikmaken, mits de tool wordt gebruikt in het kader van de landelijke fraudebestrijding en toezicht en indien akkoord is gegaan met de gebruiksvoorwaarden van Gruff. 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 teamleider toegang aanvragen tot Gruff via het IMS-autorisatiesysteem en dienen vooraf akkoord te gaan met de gebruiksvoorwaarden van Gruff. Twee medewerkers van DF&A zijn belast met de beoordeling van deze autorisatie-aanvragen waarbij, indien akkoordverklaring van de gebruiksvoorwaarden is ontvangen, extra wordt getoetst of de tool zal worden gebruikt in het kader van de landelijke fraudebestrijding en -toezicht. De onderliggende AllegroGraph-database bevat kopieën van brongegevens 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 voor-waarden op gewezen dat de gegevens uit de database niet meer actueel kunnen zijn en dat de brongegevens 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. **Dataretentie**: Verplichtingen inzake dataretentie van de output van Gruff is middels gebruiksvoorwaarden bij de eindgebruikers belegd. Wij hebben vernomen dat binnen DF&A de Archiefwet wordt nageleefd wat betreft de AllegroGraph-database. Dit is na nadere interne analyse nogmaals aan ons bevestigd. Wij hebben dit echter niet in praktijk gevalideerd.	De entiteiten betreffen objecten (auto, adres, etc.) en subjecten (natuurlijke en niet-natuurlijke personen) waartussen bestaande relaties worden getoond (fiscale partner, eigendom in periode, woonachtig in periode, etc.), zoals is vastgelegd in de bronsystemen. De verwerking ziet op het visualiseren van de aanwezige 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**: Wij hebben een memo over privacyrisico's en een WMK-toets ontvangen, maar deze stukken gaan onvoldoende in op de proportionaliteit van de gegevensverwerking.	• Binnen DF&A is geen verwerkingsdoel bepaald voor dit toolgebruik. Deze verantwoordelijkheid is belegd in de (lijn)organisatie. 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 proportionaliteit en subsidiariteit van elke verwerking te kunnen bepalen. Er wordt vertrouwd op de professionaliteit en integriteit van medewerkers om hier zorgvuldig mee om te gaan. • 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 enerzijds specifieke voorwaarden hierover zijn opgenomen in de gebruiksvoorwaarden en anderzijds door middel van monitoring op raken van VIP's in gebruik. • Relevante monitoringresultaten zoals excessief gebruik en raken VIP's wordt gemeld aan de Data Protection Officer (DPO) van DF&A. • Er heeft slechts een beperkt vastgelegde proportionaliteitstoets plaatsgevonden. Hieruit en uit onze eigen observaties en nadere toelichting van DF&A, zijn geen tekortkomingen inzake proportionaliteit vastgesteld. • Wij hebben op basis van de aan ons beschikbaar gestelde informatie onvoldoende kunnen beoordelen of voldaan wordt aan het beginsel van opslagbeperking. Hieruit volgt het risico dat mogelijk persoonsgegevens te lang worden bewaard.	WMK MM	M H

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	Marktplaatsverzoek DFEX-151				
	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 opgenomen in een 'standaard formulier' en beveiligd opgestuurd naar Marktplaats via de Belastingdienst filetransfer. Daarnaast wordt een overzicht zonder persoonsgegevens bijgehouden. 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. Het projectarchief bevat de oorspronkelijke aanvraag en het daaruit geproduceerde standaard aanvraag formulier voor Marktplaats en bevatten mogelijk (nog) persoonsgegevens. Deze worden twee jaar bewaard maar n.a.v. een AVG-scan bevat het archief alleen aanvragen van 2020. **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 alleen gegevens uitgewisseld conform het convenant, en met partijen die onderdeel zijn van dit convenant. **Dataretentie:** De informatie vanuit Marktplaats wordt na overdracht meteen verwijderd. De overige informatie die mogelijk persoonsgegevens bevatten worden binnen twee jaar verwijderd. Het product voldoet daarmee aan het beginsel van opslagbeperking.	Er worden persoonsgegevens aangeleverd van de gebruiker van Marktplaats. Het standaardformat 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:** Qua documentatie hebben wij een (verouderd) memo over de privacyrisico's ontvangen. Dit memo gaat onvoldoende in op de proportionaliteit van de gegevensverwerking.	• Mogelijk worden de advertentiegegevens van leden van het huishouden van de natuurlijke persoon waarnaar onderzoek wordt gedaan verwerkt. DF&A geeft aan dat dit risico vooral een rol zal spelen bij onvoldoende begrip van context bij de eindgebruiker. Dit zou kunnen leiden tot onjuiste aannames over de achterliggende persoon in relatie tot de advertentiegegevens. • Wij hebben op basis van de aan ons beschikbaar gestelde informatie onvoldoende kunnen beoordelen of voldaan wordt aan het beginsel van proportionaliteit. Wij hebben op basis van onze observaties echter geen zwaarwegende argumenten om te twijfelen een proportionele gegevensverwerking.	WMK MM	M L

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	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. Deze gingen gepaard met een ongekende stijging in SCAC-verzoeken. Dat was de trigger om nader onderzoek te verrichten. In dit kader is door DF&A een hypothese opgesteld op basis van inzage in correlaties en regressie(s) om de samenhang van de uitkomsten te verklaren. Hierin worden twee fases onderscheiden: • Fase 1 waarbij de hypothese wordt vormgeven en alles wat daaraan voorafgaat om tot die hypothese te komen. Dit is een gegevensverwerking in de zin van de AVG; • Fase 2 ziet toe op de verdere verwerking van (persoons)gegevens door MLC. Dit heeft er vervolgens toe geleid dat een grote fraudezaak kon worden geconstateerd. Dit was aanvankelijk een eenmalige analyse, maar inmiddels wordt deze elke drie maanden herhaald. De analyse wordt op gegevens vanuit MKB en GO uitgevoerd, waarbij personen van DF&A worden ingehuurd. Het doel van 'FIOD Berlijn – Trailer' is de preventie van fraude dat ziet op: (i) bewerking en veredeling van (ogenschijnlijk) individuele signalen; (ii) om te detecteren of er een samenhang zou kunnen zijn tussen deze individuele signalen. Dit om zodoende fenomenen, trends en ontwikkelingen in kaart te kunnen brengen. Voor zover mogelijk spelen hierbij ook aard, omvang, ernst en impact een rol. Het uiteindelijke doel, dat gestoeld is op toezicht en handhaving van de Belastingdienst, is door actueel in- en overzicht te krijgen van fraudefenomenen waarbij vervolgens gericht handhavingsregie op worden ingezet. Het primaire uitgangspunt is om deze fraude in de toekomst te voorkomen dan wel in een zo vroeg mogelijk stadium te detecteren. **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 opsporing. **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 gegevens die voor deze analyse worden gebruikt zijn in beheer van FIOD en betreffen gegevens over vastgoed, lonen en auto's, aangiftes en KvK-gegevens (handelsregister), zoals het bezitten van ontbonden rechtspersonen, de status van de afnemer en diens nationaliteit. 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 is geen GEB uitgevoerd. Het is derhalve onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	De rol binnen DF&A is niet formeel ingericht. De Belastingdienst heeft dit bevestigd, maar heeft tevens aangegeven dat de rol wel materieel is belegd. Het gaat in dit geval om de functie van 'strategische adviseur fraudepreventie'. Er zou een besloten kring moeten zijn van medewerkers die toegang tot deze gegevens zou moeten hebben; deze is echter niet bepaald. Er worden ieder kwartaal analyses uitgevoerd op gegevens die beschikbaar zijn gesteld door MKB, zonder dat hiervoor een WMK, QC en/of GEB over is uitgevoerd. Ook heeft deze gegevensuitlevering geen DFEX-nummer, waardoor het niet traceerbaar is, bijvoorbeeld voor de Functionaris Gegevens-bescherming. 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 gegevens te hebben. Anderzijds moet een bewaartermijn beredeneerd vastgesteld kunnen worden. De gegevens worden momenteel bewaard op een afgesloten deel van de Q-schijf. Wij hebben niet kunnen vaststellen of hier (de juiste) bewaar-termijnen op worden toegepast.	N	H

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	FIOD Centraal punt BTW-fraude				
	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 gegevens 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 indicatoren die in de richting wijzen van fraude, wordt vervolgens gefaseerd extra relevante informatie uitgevraagd. 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. In wezen gaat het om het verkrijgen van in- en overzicht in hoe constructies vooral worden opgezet en/of in hoeverre netwerkverbanden aanwezig zijn. Dit is gericht om na te gaan hoe deze vormen van fraude kunnen worden voorkomen, en in daarmee samenhangende 'false negatives'. Het doel is dan ook 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 opsporing. **Gegevensuitwisseling derden**: DF&A deelt geen persoonsgegevens met derde partijen – wel kennis, inzicht en ervaring.	Centraal punt BTW-fraude specialiseert zich in fraude binnen de lidstaten van de EU. Betrokkenen kunnen houders van rechtspersonen, zoals houders van leasebedrijven of frauduleuze notarissen zijn. Er worden reguliere en vertrouwelijke persoonsgegevens verwerkt. 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**: Wij hebben geen GEB kunnen bestuderen of identificeren, deze lijkt niet 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 gegevens geleverd aan MKB, zonder dat hiervoor een WMK, QC en/of GEB over is uitgevoerd. Ook heeft deze gegevensuitlevering geen DFEX-nummer, waardoor het niet traceerbaar is, bijvoorbeeld voor de Functionaris Gegevensbescherming. 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'-vereisten van deze gegevens zijn niet omschreven. Gelet op het doel van de gegevensverwerkingen van 'FIOD Centraalpunt BTW-fraude' en het risico op oneigenlijk gebruik is het nemen van passende waarborgen zoals bijvoorbeeld pseudonimisering van belang.	N	H

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	FIOD – AMLC (Trade based money laundering; FIU; No Shelter), geen DFEX-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. **Gegevensuitwisseling derden:** gegevens worden niet met externe partijen 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 extern gaan. Dit is een afweging die buiten DF&A ligt. Gegevens die in dit kader worden uitgewissel, betreft enkel gegevens die openbaar toegankelijk zijn. In dit kader is sprake van intensief contact met landelijke specialisten. Hierbij worden kennis, inzichten en ervaringen gedeeld waarbij in wezen advies wordt gegeven voor een bepaalde aanpak. **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 opsporing.	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. Betrokkenen vloeien voort uit de data-flows die samenhangen met groot-schalige fraude/misbruik. Specifiek komen de betrokkenen onder meer neer op: notarissen en houders van rechts-personen. **Proportionaliteit:** Er lijkt geen GEB te zijn uitgevoerd. Het is onduidelijk of de verwerking voldoet aan het beginsel van proportionaliteit.	**Dataretentie:** Het is onduidelijk hoelang de persoonsgegevens in kwestie worden bewaard. De processen rondom dit product is niet formeel in documentatie vastgelegd, en niet getoetst. Het is daardoor lastig aantoonbaar te maken dat persoons-gegevens van deze processen op een veilige wijze worden verwerkt.		M

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	Veelplegers team (nieuwe naam: Team aanpak risicovolle netwerken), geen DFEX-nummer aanwezig				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Veelplegers team	**Algemeen kenmerken gegevensverwerking** 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. Oorspronkelijk is vanuit (de voorloper van) EHI het project Veelplegers opgezet. Gelet op de bevindingen is een aantal jaar geleden gekozen om dit in de organisatie te beleggen in de vorm van een team. Bij bepaalde signalen zoals bijvoorbeeld turboliquidaties (wanneer een BV binnen vier maanden wordt geliquideerd) kan het gaan om dezelfde personen (Veel-plegers). De noodzaak om terug te gaan naar historische gegevens is dan aan-wezig, 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 toezichthouden. **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-nummers, IP-nummers, 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 Team risicovolle netwerken is zelf voor de persoonsgegevens verantwoordelijk. Wij hebben vernomen dat op de afgesloten Q-schijf bij DF&A (persoons)gegevens aanwezig zijn met betrekking tot deze adviesrol. Wij hebben begrepen dat deze maximaal zeven jaar worden bewaard. Wij hebben niet kunnen vaststellen of dit is vastgelegd in geformaliseerde retentierichtlijnen.	N	H

© 2021 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

3. Detailoverzicht

*R = Risiconiveau
*Doc = Beschikbare documentatie

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

	Signaalanalysepostbus, geen DFEX-nummer aanwezig				
	OMSCHRIJVING EN DOEL VAN DE VERWERKING	SOORT PERSOONSGEGEVENS EN BETROKKENEN	GEÏDENTIFICEERDE RISICO'S	Doc*	R*
Signaalanalysepostbus	**Algemeen kenmerken gegevensverwerking** Voorheen werden alle interne en externe fraudesignalen die binnenkwamen in de Signaalanalysepostbus beoordeeld en indien risico, opgewerkt en ter behandeling met advies doorgezet naar de desbetreffende informatieloketten. Momenteel gebeurt dit echter alleen met het externe signalen van TRACK Justis. De informatieverzoeken van TRACK Justis worden ook behandeld door DF&A via de analysepostbus. Deze worden na ontvangst van het informatiesjabloon via de postbus die hieronder is aangegeven, aangevuld met o.a. rapporten van boekenonderzoek, notities, etc. die van belang zijn om een compleet beeld van de (fiscale) integriteit van de betrokkenen te krijgen. Wanneer alles compleet is worden alle gegevens naar TRACK Justis verzonden opdat zij deze kunnen opwerken tot eventuele een risicomelding. TRACK Justis vraagt via een informatieverzoek de benodigde gegevens op via een informatie-sjabloon. Dit verzoek gaat naar de postbus "informatiesjabloon aanvragen_ Postbus". Afd. TRACK van Justis voert n.a.v. de ontvangen informatie van de Belastingdienst en vanuit andere bronnen(o.a. inspectie SZW, politie, UWV) een risicoanalyse uit. TRACK Justis heeft vanuit het Ministerie van JenV de opdracht om de Wet Controle op ondernemingen uit te voeren. Ze toetsten of onder-nemingen mogen worden gestart. Op basis van een convenant kan informatie bij de Belastingdienst worden opgevraagd. Als er een verhoogd risico is dan krijgt DF&A een risicomelding toegestuurd. DF&A gebruikt de ontvangen risico-meldingen 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. **Dataretentie:** Zonder sommige historische gegevens (b.v. IP-adressen) is het niet mogelijk fraude op te sporen noch tegen te gaan. Er is aan ons bevestigd dat op de peildatum 31 december jl. geen compliance-issues waren met betrekking tot het naleven van bewaartermijnen. Verzoeken van TRACK worden twee jaar bewaard en daarna opgeschoond.	De betrokkenen betreffen mensen van wie door TRACK Justis een informatie-verzoek aan Belastingdienst wordt gedaan. De persoonsgegevens die worden verwerkt, komen voornamelijk uit eigen systemen/ bronnen en die van de Kamer van Koophandel. Hierbij kunnen aangifte-gegevens, gegevens over geldstromen, nationaliteit en verblijfstitel verwerkt worden. Soms wijzen feiten op het internet in de vorm van fraudemeldingen in de richting van veelplegers. **Proportionaliteit:** Er is alleen een privacy risicoanalyse uitgevoerd, maar geen volwaardige GEB. Het is daarmee onvoldoende vastgelegd of de gegevensverwerking voldoet aan het vereiste van proportionaliteit. Zeker wanneer wordt gekeken naar mogelijk secundaire verwerkingsvormen.	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. Het convenant ziet op het primaire gebruik. **Rechtmatige grondslag:** Het beantwoorden van informatieverzoeken valt onder het convenant (en wettelijke bepalingen Wet Controle op Rechts-personen) tussen onder andere TRACK Justis en de Belastingdienst. Het verder verwerken van deze gegevens door de Belastingdienst valt hier niet onder. Een voorbeeld van verder verwerken van deze gegevens is het de aanvraag via TRACK Justis als een zelfstandig risicosignaal voor de Belastingdienst vast te leggen. Het risico bestaat dat voor deze verwerking er geen rechtmatige grondslag is. **Doelbinding:** Het primaire doel van beantwoorden van informatieverzoeken is in lijn met het doel van het convenant en wettelijke bepalingen Wet controle op rechtspersonen. Secundaire verwerkingen door de Belastingdienst geschieden niet op basis van dit convenant. Deze zijn te vinden in het memo fraude-signalen DF&A die in essentie zien op fraude-opsporing en -preventie.	MM	M

© 2021 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

Appendices

Appendix A – Lijst van interviews
Appendix B – Bestudeerde documentatie
Appendix C – Lijst van oud-EH&I-producten

Appendix A - Lijst van interviews

Wij hebben ten behoeve van het onderzoek onderstaande interviews gehouden (allen in vierde kwartaal van 2020).

Onderwerpen	Datum
Zeer Vermogende Personen	21 oktober
Gruff – Netwerkanalyse tool inclusief data; SIDN; Marktplaatslevering/marktplaatsverzoeken; Brancheinformatie (loondienst) Branche-informatie (omzetbelasting en WIA); Intranetportal/Service4u.	22 oktober
Landelijk coördinator EOS; Fraude coördinator; Fraude EOS-teams; Fraude teams Particulieren; Fraude deskundigenoverleg (FDO); Manifestgroepfraude; Werkgroep RUB (risicovolle uitbetalingen) CAP; Werkgroep faillissementsfraude (Min. JenV).	28 oktober
Schoonmaakbranche Uitzendbrache Schijnconstructies	29 oktober

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

© 2021 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
Branche-informatie	Branchecijfers WIA WMK 1.3
	Branche info LH WMK 1.2
	Branche info OB WMK 1.3
DAS-tool	Presentatie OSWO aangiftesystematiek
	Codetabel responsemessage 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 vcr 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	Gruff Logging
	2019-05-20 Voorwaarden gebruik Gruff
	Gruff-autorisaties
	Evaluatieformulier PIA Gruff
	Nota privacyrisico's Gruff
	WMK-toets EHI Relatievisualisatie v.1.0

Naam product	Documentnaam
Intranetportal Service 4u	Risicoanalyse OSINT-producten
Marktplaats	Risico's en maatregelen Marktplaats
	Marktplaatsdata
	Nota privacyrisico's Marktplaats
	Werkwijze Marktplaats vordering
	WMK-toets EHI product Marktplaats v1.0
SIDN	Sidn voorbeeld bd
	Werkwijze SIDN-aanvraag
	Nota privacyrisico's SIDN
	SIDN-data
	WMK-toets EHI SIDN
Zeer Vermogende Personen	WMK ZVPLijst 23 september 2019
	Verantwoording ZVP Top 1500
	ZVPLijst voor Vaktechniek WMK
OB Bijzondere normen	WMK-toets
Signaalanalyse-postbus	Evaluatie PIA Aanbevelingen_Signaalanalse Postbus_ondertekend
	Vragenlijst Verkenning inrichting informatiestromen
	Vragenlijst Verkenning inrichting informatiestromen beantwoording

© 2021 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 C - Lijst van producten

Naam Product/Dienst/Netwerk	DFEX
OB Telefoonverzuim	DFEX-148
Balansschulden: wordt niet uitgeleverd op dit moment	DFEX-20
OB Tweeverzuim/Veelverzuim	DFEX-19
Selfservice UCA (management informatie dashboards) voor de analyseclub voor AFP (ministerie) Fiscale Zaken. In beveiligde gegevens	DFEX-173
DG voor Fiscale Zaken – analyse fiscale politiek – convenant – Ministerie en Belastingdienst	DFEX-177
OB Bijzondere normen	DFEX-155
FIOD-account	
FIOD Berlijn – Trailer	
FIOD Centraalpunt BTW-fraude	
FIOD strategische opsporingsinformatie	
FIOD centraal punt faillisementsfraude	
FIOD – AMLC - Trade based money laundering - FIU - No shelter;	

Naam Product/Dienst/Netwerk	DFEX
FIOD Acquisitie;	
FIOD Bijzondere Taken	
FIOD IFFC Trendwatchingrapport Radicaal Samenwerken waarbij op basis van interviews (leidt tot externe publicatie);	
Veelplegers team (oude naamgeving) / Team aanpak risicovolle netwerken (nieuwe naamgeving)	
Voorlichting en Training Notariaat (KNB; extern)	
Werkgroep faillissementsfraude (Min. J&V)	
Signaalanalysepostbus	
Werkgroep RUB (risicovolle uitbetalingen)	
Landelijk coördinator EOS	
Fraude coördinator	
Fraude EOS-teams	
Fraude teams Particulieren	

KPMG © 2021 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 C - Lijst van producten

Naam Product/Dienst/Netwerk	DFEX
WAGWEU/A1 Grensoverschrijdend werk	DFEX-170
Zeer vermogende personen	DFEX-159
Gruff – Netwerkanalyse tool inclusief data	DFEX-17
DAS-tool	DFEX-179
SIDN	DFEX-153
Marktplaatslevering/marktplaatsverzoeken	DFEX-151
Branche-informatie (loondienst)	DFEX-150
Branche-informatie (omzetbelasting en WIA)	DFEX-152
Intranetportal/Service 4u	DFEX-149
Schijnconstructies (incl. - LSI: Fenomenen, risicodetectie subject. - Grensoverschrijdend werk)	
Schoonmaakbranche	DFEX-171
Uitzendbranche	DFEX-163

Naam Product/Dienst/Netwerk	DFEX
Fraude deskundigenoverleg (FDO)	
Manifestgroepfraude	
Werkgroep RUB (risicovolle uitbetalingen) CAP	
Werkgroep faillissementsfraude (Min van J&V)	
Verschillen ABS en FLG	
Gebruikelijk loon digra	
Fraude deskundigenoverleg (FDO)	
Manifestgroepfraude	

© 2021 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

De contactpersonen van KPMG voor dit rapport zijn:

[redacted]
Email: [redacted]@kpmg.nl

[redacted]
Email: [redacted]@kpmg.nl

Download on the App Store

© 2021 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden. De naam KPMG en het logo zijn geregistreerde merken die onder licentie worden gebruikt door de zelfstandige ondernemingen die lid zijn van de wereldwijde KPMG organisatie.