Belastingdienst

Rapportage DF&A

Naar aanleiding van KPMG-onderzoek oud EH&I producten

29 juni 2021

Aanleiding rapportage

› Aanleiding

Najaar 2020 heeft de Corporate Dienst Datafundamenten en Analytics (DF&A) aan KPMG opdracht gegeven onderzoek te doen. Dit onderzoek richtte zich op de producten die vanuit de voormalige afdeling EHI (Expertise en Handhaving Intelligence) in 2018 bij DF&A zijn ondergebracht, en die op peildatum 1 september 2020 operationeel waren. Het onderzoek heeft zich gefocust op de naleving van de AVG, Archiefwet en interne kwaliteits- en gedragsregels.

› Scope

De scope van het onderzoek van KPMG is afgebakend tot de Corporate Dienst Datafundamenten en Analytics zelf. Dat betekent dat KPMG interviews met betrokken binnen DF&A heeft gehouden en dat het documentatieonderzoek gericht was op de binnen DF&A beschikbare documentatie.

› Reactie MT DF&A

Het Management Team (MT) van DF&A is blij met de analyse van KMPG. Dit geeft een compleet overzicht van de huidige producten bij DF&A van oud-EHI. Door benoemen van de risico's en aandachtspunten geeft het een richting het vervolg waarin de risico's worden getoetst bij de verwerkingsverantwoordelijken en eventuele beheersmaatregelen worden genomen. De producten of diensten die aangemerkt worden met een hoog risico zijn tijdelijk stil gelegd tot de maatregen zijn gemitigeerd. Daarnaast heeft het MT twee noties bij dit onderzoek.

Het onderzoek betreft een momentopname van najaar 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 en bewaartermijnen. Met als resultaat dat op 31-12-2020 de producten uit het Onderzoeksrapport die op het exploitatieoverzicht van DF&A staan, voldoen aan de bewaartermijnen. Waar dit het geval is, wordt dit in deze rapportage aangegeven.

Door het MT van DF&A is achteraf geconcludeerd dat door de keuze om de scope te beperken tot DF&A geen volledig, en op een drietal punten onjuist, beeld is ontstaan van de onderzochte producten. Hierdoor is geen volledig beeld ontstaan van de naleving van de AVG, archiefwet en de interne kwaliteits- en gedragsregels van de producten van de voormalige afdeling EHI. DF&A maakt namelijk producten en adviezen voor, in opdracht van, en in samenspraak met, andere onderdelen van de Belastingdienst.

Vandaar dat er voor gekozen is om de constateringen van het KPMG-onderzoek met de verantwoordelijke gegevensverwerkers van de producten te delen. Samen is gekeken of de constateringen en risico's herkend worden en welke beheersmaatregelen er genomen dienen te worden. Waar constateringen vanuit het KPMG rapport worden weerlegd, is dit schriftelijke onderbouwd.

Deze rapportage is het resultaat van deze toets.

Context KPMG rapport

Doel

Het doel van het KPMG onderzoek is om te onderzoeken of de producten van oud-EH&I, die over zijn gegaan naar DF&A, voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Archiefwet en Quality Assurance (QA) kaders, inclusief de door DF&A intern gehanteerde Gouden Regels en overige van toepassing zijnde wet- en regelgeving. Tijdens het onderzoek zijn de producten ingedeeld in drie verschillende categorieën.

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.

Risico's

Bij de producten en diensten die vallen in categorie 1 worden er geen persoonsgegevens verwerkt en daarmee zijn de vereisten niet van toepassing. Voor de producten of diensten die in categorieën 2 en 3 vallen is er een omschrijving opgenomen, welke betrokkene en persoonsgegevens betrokken zijn en welke risico's er zijn geïdentificeerd. Ook is aangegeven wat de indicatie van het risiconiveau (hoog, midden en laag) gegeven.

Laag risico: er is door KPMG 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.
Midden risico: er is door KPMG 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.
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.

Het KPMG-rapport is na vaststelling in het MT van DF&A gedeeld en besproken met de betrokkenen dienstonderdelen en kaderstellende directies. De gesprekken met de inhoudelijk betrokken directies hebben tot doel gehad om:

a. Per product een gegevensverantwoordelijke aan te wijzen.
b. Per adviesdienst een opdrachtgever te benoemen.
c. Per product of adviesdienst is besproken of het risico wordt herkent, er aanvullende informatie is om het geschetst beeld aan te vullen. En wat er nodig is om de benoemde risico's te mitigeren.

Een grote onduidelijkheid rond dit onderzoek is onderstaan door het feit dat een aantal producten die benoemd zijn in het KPMG-rapport feitelijk geen producten zijn maar adviesdiensten. En dat er hier geen sprake is van gegevensverwerkingen. Daarmee zijn deze producten langs een meetlat gelegd die niet past bij adviesdiensten. Per product zal toegelicht worden wat de aanvullende bevindingen zijn op dit vlak.

Hieronder treft u een uiteenzetting van de 18 producten en diensten, risico's, aanvullende bevindingen en mitigerende maatregelen die vallen onder categorieën 2 en 3.

Producten en diensten overzicht oud EH&I

Nr.	Product*	Product-kenmerk	Risico aanduiding KPMG rapport	Verwerkings-verantwoordelijke	Aanvullende bevinding i.o.m. verwerkingsverantwoordelijke	Mitigerende maatregelen
1	FIOD Berlijn- Trailer	Geen product	Hoog	n.v.t	Dit is geen product, er is geen sprake van gegevensverwerking en geen sprake van opdrachtgeverschap door FIOD. Dit is geconstateerd door experts van DF&A en FIOD en bevestigd door MT DF&A en FIOD. Wel is geconstateerd dat tussen DF&A en FIOD kennis en ervaring uitgewisseld. Dit zijn advieswerkzaamheden. Er worden hierbij geen persoonsgegevens gedeeld.	De advieswerkzaamheden worden door DF&A in Q3 geformaliseerd en opgenomen in de productcatalogus. Het streven is om in Q4 de advieswerkzaamheden te implementeren en daarmee te laten voldoen aan de privacy- en kwaliteitseisen. (Gereed 1 januari 2022)
2	FIOD Centraalpunt Btw-fraude	Geen product	Hoog	n.v.t	Dit is geen product, er is geen sprake van gegevensverwerking en geen sprake van opdrachtgeverschap door FIOD. Dit is geconstateerd door experts van DF&A en FIOD en bevestigd door MT DF&A en FIOD. Wel is geconstateerd dat tussen DF&A en FIOD kennis en ervaring uitgewisseld. Dit zijn advieswerkzaamheden. Er worden hierbij geen persoonsgegevens gedeeld.	De advieswerkzaamheden worden door DF&A in Q3 geformaliseerd en opgenomen in de productcatalogus. Het streven is om in Q4 de advieswerkzaamheden te implementeren en daarmee te laten voldoen aan de privacy- en kwaliteitseisen. (Gereed 1 januari 2022)
3	Veelplegers team/ Team aanpak risicovolle netwerken	Geen product	Hoog	MKB	Dit is geen product. Signalen die verkregen worden, worden binnen de Belastingdienst doorgespeeld naar de competente kantoren. Dit zijn advieswerkzaamheden.	Proportionaliteit: De GEB risicovolle netwerken valt onder verantwoordelijkheid van MKB. Deze is in bewerking en aangepast op basis van de bevinding van KPMG. In de GEB is de rol van DF&A nu opgenomen. De privacy officer van DF&A heeft hulp aangeboden om deze rol van DF&A in de GEB de komende tijd verder aan te scherpen. (Een gereeddatum kan hiervoor nu niet worden gegeven.) De advieswerkzaamheden worden door DF&A in Q3 geformaliseerd en opgenomen in de productcatalogus. Het streven is om in Q4 de advieswerkzaamheden te implementeren en daarmee te laten voldoen aan de privacy- en kwaliteitseisen. (Gereed 1 januari 2022)

* Niet alles wat in deze kolom genoemd wordt is daadwerkelijk een product. Daarnaast dekt de naamgeving in een aantal gevallen niet de lading.

Nr.	Product*	Product-kenmerk	Risico aanduiding KPMG rapport	Verwerkings-verantwoordelijke	Aanvullende bevinding i.o.m. verwerkingsverantwoordelijke	Mitigerende maatregelen
4	DAS- tool	Geen product	Midden	n.v.t.	Dit is geen product maar een tool. Deze tool geleidt gegevens vanuit de BD-omgeving naar standalone pc's. De informatie uit deze tool wordt gebruikt door MKB en GO ter controle. De tool vervult een belangrijke taak in het gehele loonheffing proces. Het is niet mogelijk om dit product uit te schakelen zonder dat er een alternatief voor handen is. Momenteel is MT MKB aan het uitzoeken (in overleg met GO en Particulieren) wie gaat optreden als verwerkingsverantwoordelijke.	Uiterlijk Q2 zal er een verwerkingsverantwoordelijke zijn. Zodra er een verwerkingsverantwoordelijke is kan dit dienstonderdeel de mitigerende maatregelen nemen.
5	Zeer vermogende personen	DFEX-159	Midden	GO	De bevindingen van KPMG worden herkend door GO.	De query- codes zijn inmiddels afgeschermd. Alle codes zijn naar een eigen, afgezonderd werkgebied verhuisd. Zo is de toegang voor medewerkers beperkt. (Gereed) Onder verantwoordelijkheid van de directie Grote Ondernemingen wordt er momenteel een GEB opgesteld. (De verwachting is dat de GEB in Q4 wordt afgerond.)
6	Gruff Netwerkanalysetool	Geen product	Midden	n.v.t.	Dit betreft geen analysetool is Ad risico 1, 2, 4, 5: bevinding wordt herkend Ad risico 3: bevinding wordt niet herkend, het is juist een mitigerende maatregel dat indien Vips worden 'gehit', de Data- en Privacy Officer (DPO) op de hoogte wordt gesteld.	In Q3 2021 vindt door DF&A de doorontwikkeling van de tooling plaats die gaat voldoen aan de standaarden en richtlijnen van DF&A. Dat houdt in dat er een visualisatietool ontwikkelt gaat worden die dezelfde inzichten biedt vanuit een analytics benadering. Bij de ontwikkeling worden de bevindingen van het KPMG onderzoek gemitigeerd. Tot die tijd worden de geïdentificeerde risico's geaccepteerd. (Gereed 1 oktober 2022)
7	FIOD - AMLC	Geen product	Midden	n.v.t.	Dit is geen product, er is geen sprake van gegevensverwerking en geen sprake van opdrachtgeverschap door FIOD. Dit is geconstateerd door experts van DF&A en FIOD en bevestigd door MT DF&A en FIOD. Wel is geconstateerd dat tussen DF&A en FIOD kennis en ervaring uitgewisseld. Dit zijn advieswerkzaamheden. Er worden hierbij geen persoonsgegevens gedeeld.	De advieswerkzaamheden worden door DF&A in Q3 geformaliseerd en opgenomen in de productcatalogus. Het streven is om in Q4 de advieswerkzaamheden te implementeren en daarmee te laten voldoen aan de privacy- en kwaliteitseisen. (Gereed 1 januari 2022)

Nr.	Product*	Product kenmerk	Risico aanduiding KPMG rapport	Verwerkings-verantwoordelijke	Aanvullende bevinding i.o.m. verwerkingsverantwoordelijke	Mitigerende maatregelen
8	Signaalanalyse Postbus	DFEX- 157	Midden	MKB	De convenant ziet er op toe hoe de signalen van- en naar Track Justis over en weer in een goed proces verloopt die in de convenant is beschreven. Bovendien komen de mails wel versleuteld binnen, alleen twee medewerkers kunnen zien wat de signalen zijn, omdat zij bij de encryptie software kunnen.	Momenteel wordt er o.a. door MKB gewerkt aan een tijdelijke oplossing ten behoeve van de rechtmatige grondslag. Waarna gewerkt wordt aan definitieve oplossing met de gewenste architectuur. 2. Er loopt onder verantwoordelijkheid van MKB al geruime tijd een GEB op het signaalproces MKB, GO en P. DF&A is in de concept GEB aangemerkt als interne verstrekker. 3. De verschillende signalenstromen die allen in de postbus terechtkomen, zullen allen afzonderlijk worden beschreven inclusief doelbinding, eigenaar en proces.
9	FIOD Bijzondere Taken	Geen product	Midden	n.v.t.	Dit is geen product, er is geen sprake van gegevensverwerking en geen sprake van opdrachtgeverschap door FIOD. Dit is geconstateerd door experts van DF&A en FIOD en bevestigd door MT DF&A en FIOD. Wel is geconstateerd dat tussen DF&A en FIOD kennis en ervaring uitgewisseld. Dit zijn advieswerkzaamheden. Er worden hierbij geen persoonsgegevens gedeeld.	De advieswerkzaamheden worden door DF&A in Q3 geformaliseerd en opgenomen in de productcatalogus. Het streven is om in Q4 de advieswerkzaamheden te implementeren en daarmee te laten voldoen aan de privacy- en kwaliteitseisen. (Gereed 1 januari 2022)
10	Schoonmaak branche	DFEX- 171	Laag	MKB		Geen risico's geconstateerd door KPMG.
11	Schijn-constructies	DFEX- 170	Laag	MKB		Geen risico's geconstateerd door KPMG.

Nr.	Product*	Product kenmerk	Risico aanduiding KPMG rapport	Verwerkings-verantwoordelijke	Aanvullende bevinding i.o.m. verwerkingsverantwoordelijke	Mitigerende maatregelen
12	Uitzendbranche	DFEX- 163	Laag	MKB		Geen risico's geconstateerd door KPMG.
13	OB telefoonverzuim	DFEX- 213	Laag	MKB	Dit product is inmiddels omgebouwd naar het product Verzuimaanpak (DFEX213)	Na de ombouw voldoet het nieuwe product aan de standaarden en richtlijnen en daarmee aan de bewaartermijnen. Dit is inmiddels het geval.
14	OB tweeverzuim / Veelverzuim	DFEX- 213	Laag	MKB	Dit product is inmiddels omgebouwd naar het product Verzuimaanpak (DFEX213)	Na de ombouw voldoet het nieuwe product aan de standaarden en richtlijnen en daarmee aan de bewaartermijnen. Dit is inmiddels het geval.
15	OB Bijzondere normen	DFEX-155	Laag	MKB		Het product voldoet inmiddels aan de gestelde bewaartermijnen. (Gereed)
16	Branche-informatie	DFEX-150-152	Laag	MKB	MKB is voornemens om op te treden als verwerkingsverantwoordelijke. MKB zorgt er voor dat er in Q2/Q3 formeel uitspraak wordt gedaan door het MT van MKB.	Product voldoet uiterlijk Q3 2021 aan de bewaartermijnen.
17	SIDN	DFEX-153	Laag	?	Alle gebruikers zijn benaderd met de benaderd wie verwerkingsverantwoordelijke is. Hieruit is gebleken dat het product nu geen verwerkingsverantwoordelijke heeft.	Uiterlijk juli 2021 is een verwerkingsverantwoordelijke aangewezen. Zo niet, zal het product worden uit gefaseerd.

Nr.	Product*	Product kenmerk	Risico aanduiding KPMG rapport	Verwerkings-verantwoordelijke	Aanvullende bevinding i.o.m. verwerkingsverantwoordelijke	Mitigerende maatregelen
18	Marktplaatsverzoek	DFEX-151	Laag	n.v.t	Alle gebruikers zijn benaderd wie verwerkingsverantwoordelijke is. Hieruit is gebleken dat het product geen verwerkingsverantwoordelijke heeft en om die reden uit gefaseerd zal worden met ingang van 1 juli 2021.	Vanwege de uitfasering zijn de risico's niet langer aanwezig.