met de collega's die we er nu bij hebben gevraagd. Om in die tijdlijn van 2013 – 2020 beter duiding te kunnen geven over hoe het gegaan is en hoe het nu is ook vooral.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik zal even toetsen of dat klopt.

Persoonsgegevens

Ik weet niet beter dan dat stuk wat aan u toegestuurd is vorige week en wat nu ook meegestuurd is als stuk de andere kant op. Dat is de enige tijdlijn die wij kunnen reproduceren. Veel gedetailleerder dan dat gaat het niet worden.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

In tekst. Ik zou niet weten hoe we dat zouden moeten detailleren.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Het is even zoeken van wat de beste vorm is. Zullen we ook afspreken dat jullie gewoon tussendoor vragen stellen over waar jullie dan nog nieuwsgierig naar zijn of graag willen weten? Ik denk dat ik gewoon even het woord geef aan de betrokken collega's die ik erbij uitgenodigd heb om context te geven over hoe het zit. Wat ik net ook al aangaf, wij vonden het lastig om een heel duidelijk beeld te geven over hoe het met die autorisaties is gegaan omdat eigenlijk door de tijd heen de organisatie erg veranderd is. Het centrale deel zoals wij dat nu hebben, dat hadden wij in 2013 nog niet. Vandaar dat het lastig terug te halen is. Maar ik denk dat ik het beste als eerste het woord kan geven aan Persoonsgegevens want die kan die uitleggen hoe het nu is eigenlijk.

Persoonsgegevens

Ik denk vooraf even goed om te snappen dat de keten Generiek Kantoor en Toezicht een typisch andere keten is dan de gemiddelde andere 13, 14 die je ook in het plaatje ziet staan. In deze keten werken allerlei business partners met IV en met analytics samen in een bepaald domein. En dit is het domein Kantoor en Toezicht en daar vallen in ieder geval

allerlei toezichtvoorzieningen onder waarmee medewerkers in de controle en handhaving aan het werk gaan. Daar valt dus ook een applicatie onder als de Fraude Signalering Voorziening en nu de opvolger de tijdelijke signalering voorziening. Dus dat valt echt wel in dit domein. Het is een generieke voorzieningenketen, het is heel IT georiënteerd. Dus dat betekent dat wij weinig in de uitvoering doen. Je hebt ook ketens zoals BBK, Beroep Bezwaar en Klachten en nog een aantal anderen die ook echt dat uitvoeringsgedeelte veel meer in de keten hebben gebracht en daar ook op monitoren. Ik monitor in mijn keten niet met de ketenpartners op hoeveel boekenonderzoeken heb je gedaan? Hoeveel signalen heb je? Dat is niet wat wij in deze keten doen. Wij zijn wel opgesteld om het hele fundament van de voorzieningen, inclusief de processen die in dat toezicht zijn en de voorzieningen eronder, om dat totaal te vernieuwen. Dus dat fundament dat zetten wij generiek neer. Dat is het belangrijkste doel voor deze keten.

Dat betekent dus ook dat wij een beweging aan het maken zijn van allerlei oude voorzieningen waaronder dus FSV wat nu uit de lucht is gehaald, naar nieuwe voorzieningen die helemaal up to date zijn. Ook qua privacy by design, need to know enz. Ik moet daar wel bij vertellen, dat zal Persoonsgegevens ook kunnen onderschrijven, dat ons landschap zeer divers is, dat ik zeker nog zo'n 70 voorzieningen heb die in het oudere landschap zitten, die ook gemaakt zijn in een heel ander tijdsgewricht. De timing waarin FSV ooit gemaakt is, was heel anders en voldeed dus ook niet aan allerlei AVG-normatieken die we nu sinds een paar jaar hebben. Het is ook heel lastig om al die oude voorzieningen daar in voldoende mate in de techniek up to date te krijgen. Dus wij kiezen ook heel bewust 'wat moet nog handmatig aangevuld worden met maatregelen en waar kunnen we dingen echt stop zetten'. Bijvoorbeeld een export functionaliteit, dat willen wij ook niet. Dat is heel lastig om te controleren. Daar zijn we nu ook mee bezig omdat allemaal stop te zetten. Dus dat zijn zaken waar we nu mee bezig zijn, waar we middenin zitten.

Het betekent ook dat het gedeelte waar GKT over gaat, is dus ook met name technisch en functionele beheer van de voorzieningen. Niet zozeer het proces daarvoor. Als het gaat om autorisaties en het verlenen van autorisaties, dan is dat een verantwoordelijkheid en dat is eerder al gedeeld en dat staat ook in het stuk, wat ligt in de lijnorganisatie. Wij ondersteunen wel en dat zien jullie ook in de matrix die is teruggestuurd, als er nou specifieke vragen zijn over 'doe mij een analyse over hoe dat nou zit met die autorisaties in FSV bijvoorbeeld', dan kunnen wij daar een bijdrage aan doen. Dat hebben wij ook gedaan. Persoonsgegevens is volgens mij ook door jullie gehoord. Die heeft daar ook een toelichting op gegeven vanuit de techniek. Het is ook logisch dat wij niet zomaar bij die systemen kunnen als ketenbureau of als IV partner omdat we dan, dan heb je al een breuk met de beveiliging. Dat is op zich heel logisch dat we dat niet hebben.

Als het gaat om het koppelen aan FSV, wij hebben ooit in 2013, is de overslag van een nog oudere voorziening naar FSV gedaan. Dat hebben jullie ook al genoteerd. Op dat moment is ook gekeken naar de autorisaties en is ook gestart met het onder IMS brengen. Ik zie in de notitie die daarbij ligt, dat dat eind 2017 gedaan zou zijn. Maar mijn beeld is, en dat heb ik ook wel berichtgeving van, dat dat wel eerder is. Maar dat zal Persoonsgegevens misschien beter kunnen duiden wanneer FSV daadwerkelijk onder IMS is gebracht. Want ik heb er berichten van dat dat tussen business en IV destijds in 2013 met de toenmalige IMS-houder, laat ik het dan maar zo zeggen, in IMS is gebracht.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Wat mij betreft wel.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik zal dat afstemmen nog met MKB, want dat is een traject geweest waar met name MKB als business partner met IV, de organisatie die toen over IMS ging, is dat opgepakt. Die kan ik via die lijn doen.

Qua proces, eigenlijk zou het goed zijn als Persoonsgegevens dat zo bevestigt, is dat met de omslag naar IMS ook heel nadrukkelijk is gekozen voor dat je als medewerker in het toezicht rollen toegekend krijgt of een profiel toegekend krijgt waarin passend bij jouw werk je autorisaties voor systemen krijgt. Dan gaat het dus niet meer op welke manier dan ook, los van iemand in de lijn, per mailbox, dat er dan gevraagd wordt van 'ik wil voor FSV deze autorisaties'. Nee, je hebt gewoon bij een bepaalde medewerker past een bepaald profiel. Op basis van dat profiel krijg je autorisaties op een groter geheel van applicaties die je nodig hebt om je werk te doen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Ja. Ik denk dat Persoonsgegevens dit ook nog wel heel goed kan uitleggen zo meteen.

Persoonsgegevens

Ja, precies. Wat je bij FSV ziet, is dat daar drie lagen waren. Dat is volgens mij ook toegelicht door Persoonsgegevens Je hebt rollen in IMS, een verfijning in FSV van die rol. Dus bijvoorbeeld in IMS, dat zal Michel dan zo meteen kunnen vertellen, staat er raadpleging. En je ziet het ook, ik zit te wijzen naar mijn computer wat heel onhandig is, dat gaan jullie natuurlijk niet zien. Maar in de Excel die daarbij zit, staat ook welke rollen je allemaal hebt in FSV. Dan heb je misschien raadpleging, maar dan zijn er ook use cases waar je bij een rol dan ook nog autorisaties toe hebt. Als slot was er de derde laag, dat op moment dat je geautoriseerd bent voor IMS FSV, dat je dan pas technisch toegang krijgt tot FSV zelf. Dus dat zijn de drie lagen die wij daar kennen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, ik verwijs naar een document wat teruggekomen is <*er wordt verwezen naar het document '30 Rollen waarin FSV-permissie aanwezig is.xls'*>. Ik zal de naam van het tabblad noemen: 'autorisatiematrix'. Daarin zie je de use cases. Dat is FSV-taalgebruik. Die use case. Dat is ook eerder al uitgelegd. Ook qua logging is daar het een en ander over toegelicht. Dat je wel kunt zien wie een use case benadert in FSV, achteraf. Dat wordt gelogd. Maar wat er precies gedaan wordt in FSV bij die use case, dat kan je niet terughalen. Als het geheel verwijderd wordt, dan zie je het, dus als je de hele use case verwijdert. Maar als jij een stukje in die use case verwijdert, bijvoorbeeld een tekstveld leeg haalt, dat zie je niet. Dat is ook in het KPMG-onderzoek eerder al benoemd.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Het was in ieder geval Persoonsgegevens

Persoonsgegevens

Het zou fijn zijn dat dit ook uitgelegd is.

Persoonsgegevens

Het is uitgelegd in de sessie waar ik bij was.

Persoonsgegevens

Persoonsgegevens kun je ook nog wat vertellen over het moment van het wanneer wij het uitgezet hebben?

Persoonsgegevens

Het is twee keer uitgezet, FSV. Beide keren, daar is ook wel mailverkeer van. Volgens mij is dat ook wel al aan de orde geweest. De eerste keer was rondom de invoering van de AVG, dus in mei 2018 is die stil gezet. Omdat we toen inderdaad zoveel gebruikers in dat systeem hadden. Dat werd ook gesignaleerd vanuit onderzoek vanuit onze IV-organisatie. En het tweede punt was de export functionaliteit die er in zat. En op beiden is op dat moment, in overleg met de betrokken business partners, waaronder MKB, omdat dat een grootgebruiker is van deze voorziening, is gezegd 'dat moet naar beneden', hebben we analyse uitgevoerd om die 5.000 naar zo'n 1.000 terug te brengen. Dat is ook, in de Kamerbrief staan de precieze aantallen, maar is dat teruggebracht.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

We hadden natuurlijk verschillende onderzoeken lopen vanuit de AVG. Vlak voordat die datum inging, zijn er een aantal extra checks geweest. Dit is daar onder andere, het is niet helemaal van vlak daarvoor. Ik zou echt terug moeten kijken in de stukken of ik dat terug kan herleiden wanneer dat precies op kwam, maar tegen mei 2018. En toen is gezegd van: 'zoveel gebruikers, plus die exportfunctionaliteit, daar moet op ingegrepen worden'. Daar heeft de ketenvoorzitter uiteindelijk met de betrokken businessvertegenwoordiger, dat was de directie MKB onder andere, is gezegd 'wij zetten het stop'. Dat is ook gebeurd. En daarna is het weer, na aanpassingen in autorisaties en exportfunctionaliteit, beide zijn beperkingen doorgevoerd, is het uiteindelijk weer in de lucht gebracht. Ook weer op aangeven van de ketenvoorzitter na afstemming met de vragende business. Die het graag weer wilde ter ondersteuning van hun bedrijfsproces.

De tweede keer stopzetten, dat is dit voorjaar. Daar kan ik heel weinig over zeggen. Maar uiteindelijk is daar ook voor gezegd 'het systeem moet uit de lucht'. Daar heeft de ketenvoorzitter uiteindelijk de opdracht toe gegeven en is het systeem uit de lucht gehaald.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is ook gedaan.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Nee. Volgens mij is het zo dat, maar dat kan Persoonsgegevens beter uitleggen, dat het aanpassen van die profielen in IMS best wel een behoorlijke klus is en ook complex. Wat er is gebeurd, is dat in FSV zijn die autorisaties aangepast. Dus van 5.000 naar 1.000 en dan zou je het in IMS nog kunnen hebben, maar dan kom je niet in FSV. Je hebt dan die link, die is ook aangepast. Dan heb je twee lagen, daarin is het aangepast. De FSV zijn de autorisaties aangepast en de link is aangepast. Dat staat ook in die mail van mevrouw Persoonsgegevens

Persoonsgegevens

Is het dan nu een logisch moment om Persoonsgegevens te vragen of hij op IMS een toelichting kan geven Persoonsgegevens

Persoonsgegevens

Ja, ik denk dat het wel goed is dat qua procesgang dat het wel zo is, dat het autorisatieproces, daar heeft Persoonsgegevens zijn club natuurlijk het nodige in te doen. Maar dat is wel een lijnverantwoordelijkheid. Dat is wel belangrijk dat dat goed in de boeken komt te staan.

Persoonsgegevens

In de eerste plaats het proces van logische toegang. Ik zit hier niet als specialist in relatie tot FSV. Mijn betrokkenheid is puur vanuit het proces wat voor de hele Belastingdienst geldt en voor alle applicaties, hoe wij zorgen dat wij op een gecontroleerde manier medewerkers van de juiste autorisatie voorzien. En dat proces logisch toegangsbeheer is onderdeel van de keten Bedrijfsvoering. Dus dat is ook een andere keten dan de keten waar Inge in werkzaam is. Wij beschouwen dit als een onderdeel van de bedrijfsvoering.

In IMS worden er rollenmodellen gemaakt. Daar werd net al aan gerefereerd. Feitelijk is het vakjargon voor het mechanisme wat wij hanteren, is een rolled based access control. In logisch toegangsbeveiligingsland betekent dat eigenlijk dat je op basis van een rol die je hebt in de organisatie, een rol is toch anders dan een functie die je hebt in SAP bijvoorbeeld. Want een medewerker die heeft maar één functie, maar die kan in die functie misschien wel meerdere rollen hebben. Rollen hoeven niet per se een één-op-één relatie te hebben met wat een medewerker doet.

Wat we wel doen in zo'n rollenmodel is voor een rol, dus voor bij elkaar behorende autorisaties om een bepaalde rol uit te kunnen voeren, die proberen wij in dat rollenmodel zoveel mogelijk te groeperen. Dus waar [Persoonsgegevens] straks ook aan refereerde; het kan dus zijn dat je toegang krijgt tot een bepaalde rol, dat daar een raadpleeg functie voor FSV in zit en misschien nog wel een raadpleegfunctie voor zes andere applicaties. Die dan op basis van die rol geacht worden bij die medewerker noodzakelijk te zijn. Wij kunnen vanuit het LTB proces niet beoordelen van wie welke autorisaties mag hebben. Dat is een verantwoordelijkheid van de business in samenspraak met de eigenaar van een applicatie. In onze organisatie is de manager verantwoordelijk voor de autorisaties die zijn medewerker krijgt. Die manager is ook degene die in IMS aan zijn medewerker rollen toekent. Maar zo'n manager kan ook een rol toekennen waar die mogelijk niet noodzakelijk is voor zijn medewerker en waar iemand die verantwoordelijk is voor als eigenaar van het proces een controlerende taak krijgt voordat de rol daadwerkelijk aan een medewerker wordt toegekend. Dus het is niet zo dat een manager zijn medewerker alle rollen die in het rollenmodel staan, ook daadwerkelijk kan toekennen. Het kan soms ook zo zijn, dat is veel gevallen zo, dat rollen beoordeeld moeten worden door bijvoorbeeld iemand die eigenaar is van de inhoud van een rol. En dat zal met de algemene rollen, waar ik net aan refereerde, waar dingen bij elkaar gevoegd zijn om in één rol meerdere autorisaties in meerdere systemen te krijgen zal het minder aan de orde zijn. Maar je kan je ook voorstellen dat daar in teams medewerkers een rol hebben en dat er een enkele medewerker misschien nog een speciale taak heeft. En dat hij daarvoor een soort bijzondere taak, wat ook een verschijningsvorm van een rol in IMS, naast de standaard rol die je nodig hebt, dat je dan aan een enkeling binnen een team ook een bijzondere rol geeft. Bijvoorbeeld als er een team is waar zaken afgehandeld worden en waarbij een individuele medewerker misschien VIP posten moet behandelen bijvoorbeeld, dan zou je in theorie kunnen bedenken dat je één of twee medewerkers via een rol bijzondere taak dus autorisaties geeft voor die specifieke VIP posten en dat je het behandelen van alle andere zaken rond een dergelijke applicatie, aan iedereen in het team geeft.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Grofweg hebben we daar twee varianten in. Er zijn een aantal rollen die wij in het rollenmodel van IMS zo gedefinieerd hebben, dat die afhankelijk zijn van de plek die een medewerker in de HR-administratie inneemt. Wij hebben IMS, het autorisatiesysteem, heeft een automatische koppeling met ons personeelsbestand. Je kan je voorstellen dat er mensen zijn die in een bepaalde functie zitten of in een bepaald team waarvan je zegt 'die mensen die in dat team zitten, die hebben altijd bepaalde autorisaties nodig'. Dan zijn wij in staat om op basis van een, wat we in IMS termen een 'rule' noemen, een regel, dat we kunnen zeggen van 'als jij in team A zit van onderdeel douane en je hebt in SAP een bepaalde functie, dan krijg je automatisch één of meerdere rollen toegewezen'. Dat is eigenlijk een roltoewijzing die automatisch plaatsvindt zonder dat een manager daar iets voor hoeft te doen op basis van jouw plek in de organisatie en de functie die je vervult in de organisatie. Dat is één.

Het leeuwendeel van de rollen wordt niet op deze manier toegekend, maar die worden inderdaad door de manager van de medewerker via IMS, waar een manager toegang toe heeft. De manager krijgt in het rollenmodel toegang tot die rollen waar die in principe medewerkers aan mag allokeren. Dat zijn veelal de rollen van het organisatieonderdeel waar de manager werkzaam is. Een manager van douane kan niet zo maar een medewerker aan een rol van de FIOD koppelen om maar een voorbeeld te geven. Dus een manager krijgt niet alle rollen die er in IMS zitten te zien. Daar zit al een technische filtering in, dat er rollen bij een manager zichtbaar worden die mogelijk voor zijn medewerkers van toepassing zijn. Die manager zal dan op basis van de rol van zijn medewerker, zal die dan één of meerdere van die rollen of bijzondere taken, wat feitelijk ook rollen zijn, toewijzen aan een medewerker, geautomatiseerd. En dan al naar gelang de aard van de rol of daar nog een extra goedkeuring op zit, zal voor dat de autorisaties daadwerkelijk worden toegekend, zal die eerst nog via een loket komen waar bijvoorbeeld een eigenaar van een proces of de eigenaar van de applicatie daar iets over kan zeggen, voordat die autorisaties daadwerkelijk worden goedgekeurd. Dus het kan zijn dat een manager iemand een rol geeft, maar dat die medewerker die toch niet krijgt omdat de beoordelaar die daar achter zit zegt 'dat heeft jouw medewerker helemaal niet nodig, dat gaan we dus niet doen'.

Persoonsgegevens

Kun je het iets mee toespitsen naar FSV misschien?

Persoonsgegevens

Ik heb geen inzicht paraat over hoe de FSV er uitgezien heeft in IMS. Ik heb wel recentelijk in IMS gekeken en ik heb gezien dat er nu nog maar een beperkt aantal rollen zijn waarmee autorisatie voor FSV uitgereikt kunnen worden. Die rollen, daar zit allemaal zo'n goedkeurders attribuut op. Dus het is niet zo dat er op dit moment mensen aan FSV gekoppeld kunnen worden door een manager zonder dat daar specifieke goedkeuring op heeft plaatsgevonden door iemand die namens FSV dat kan beoordelen.

Persoonsgegevens

Dit is de recente situatie?

Persoonsgegevens

Ja, dat klopt.

Persoonsgegevens

Kan je ook iets vertellen over hoe de IMS inrichting in de stapjes terug is geweest en in hoeverre we daar dan nog inzicht in kunnen krijgen of uit kunnen halen?

Persoonsgegevens

Wij kunnen op twee soorten manieren rapportages verzorgen uit IMS. Feitelijk worden alle acties die in IMS uitgevoerd worden, waar het meestal managers zijn maar ook acties die mijn collega's als functioneel beheerders bijvoorbeeld uitgevoerd hebben. Alle acties worden in IMS gelogd als een event, als een technische handeling. Daar kunnen wij informatie uit halen. Dus ook de historische logging van wanneer heeft iemand een rol toegewezen aan iemand. Dat noemen wij audit informatie feitelijk. Daarnaast hebben wij een systeem dat wij periodiek onze klanten middels BI-rapportages informatie geven over de situatie van nu. Dus je kan je bijvoorbeeld voorstellen, wij leveren wekelijks verschillende soorten rapportages op. Die maken dan een snapshot uit hoe het nu in IMS zit. Dat is de realtime situatie. Die realtime situatie die kan dan bijvoorbeeld weergeven van welke medewerkers hebben welke rollen gezeten of welke permissies. Er zijn allerlei varianten van BI-rapportages mogelijk. Wat een belangrijke kanttekening is bij dit soort rapportages, is dat je op basis van die rapportages niet volledig kan traceren wanneer heeft iemand toegang gehad tot een bepaalde applicatie. Je kan je voorstellen als er een rapportage is die iedere week opgeleverd wordt, bijvoorbeeld op maandag, dan leveren wij een rapportage op met dit is de situatie zoals die vandaag in IMS zit. Dan zou het in theorie kunnen dat er morgen een medewerker gekoppeld wordt aan een rol en dat die er overmorgen weer afgehaald wordt. Dan vind je hem de week daarop in de rapportage die allocatie niet terug omdat de week daarop een moment is van die dag zelf. Als je dus daadwerkelijk wilt traceren van wie heeft wanneer aan welke autorisaties gezeten, dan zullen we dus moeten gaan spitten in het logbestand wat ik in eerste voorbeeld aanhaalde. Waar wij dus alle handelingen die in IMS gedaan worden in bewaren.

Er zijn twee dingen die ons daar op dit moment in beperken. Eén is heel helder. Dat is namelijk de wetgeving die ons voorschrijft op basis van de archiefwet dat wij onze informatie niet langer dan vijf jaar mogen bewaren. Die logging informatie, als wij ze uit IMS logging kunnen halen, die zal niet verder terug gaan dan nu vijf jaar geleden. Dynamisch wordt die informatie zo gehouden, dat alles wat ouder is dan vijf, wordt uit onze database verwijderd. Dus als het gaat over FSV. Ik heb begrepen dat FSV vanaf 2013 actief is. Ik hoor ook twee verschillende data Persoonsgegevens eerde al, in het verslag wordt er geschreven over eind 2017. Wij hebben in de logging wel records met FSV aangetroffen die al van eerdere datum zijn. Wij konden niet verder terug dan december 2015. Wat dat is nu vijf jaar geleden. Daar hebben we wel records aangetroffen van FSV.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Wat dat betekent, dat is misschien wel even technisch. Om die informatie uit die database te halen, dat is wat anders dan de rapportages die wij wekelijks opleveren. Om op die logging database waar allemaal events in zitten, wat feitelijk allemaal regeltjes zijn. Waarvan nu heeft een manager op een knop gedrukt waardoor user x gekoppeld is aan rol y. Maar daar zitten dus ook logische verbanden in. We moeten die events aan elkaar knopen om een logische regel te krijgen van op die dag heeft die manager die medewerker gekoppeld aan

een rol van FSV. Wat ik ter voorbereiding op dit gesprek even gecheckt heb met mijn collega's, is dat wij in ieder geval de term FSV tegenkomen in de database. Maar ik heb nog geen inspanningen laten doen om daar ook logische informatie voor FSV uit te halen. Want dat is erg complex. Dat heeft met de techniek te maken. Wij hadden eerst een andere structuur van de database, waar die informatie in zit en een andere tool die wij gebruiken om auditinformatie uit IMS te halen. Wij hebben recentelijk besloten dat we dat proces gaan migreren naar een andere tool die wij daarvoor gebruiken. Daarvoor is de structuur van de database die aan IMS zat, die is omgebouwd naar een andere structuur waar die nieuwe tool mee kan praten. Die nieuwe tool dat is 'Splunk', voor the record. Misschien dat jullie daarvan weleens van gehoord hebben.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

De database structuur van Splunk, die is technisch gezien heel anders dan de database structuur van de audittool die wij tot voor kort gebruikten. Wij hebben nu een migratieslag gedaan. Wij hebben nog wel steeds die vijf jaar aan informatie van IMS beschikbaar. Alleen wij zitten op dit moment in een fase waarin wij om het met Splunk er op een logische manier uit te krijgen, nog werk moeten verrichten om dat voor elkaar te krijgen. Daar moet een zogenaamd dashboard voor gemaakt worden. Daar is technische kennis voor nodig en LTB kennis voor nodig om die dashboards te maken. Dus op korte termijn kan ik niet bijvoorbeeld een rapportage uitdraaien van 'geef mij maar eens alles wat je kan vinden over FSV sinds 2015'. Dat gaat op dit moment technisch gezien niet lukken. Dat heeft dus te maken met die transitieperiode waar we net in zitten. In de techniek van de manier waarop wij de auditgegevens tevoorschijn toveren.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Technisch gezien is dat mogelijk. Dan wel met de restrictie dat, ik heb navraag gedaan, de rapportages, die statische BI-rapportages waar ik het dan over heb, wat Excel overzichten zijn overigens. Dus dat overzicht wat u van Persoonsgegevens hebt ontvangen, dat is waarschijnlijk ook één van onze rapportages geweest. Onze technische informatie gaat terug tot september 2016. Dus uit die rapportages kan ik geen oudere informatie opleveren dan vanaf september 2016. Wat ik daarbij ook nog moet aanmerken, is dat er toen in die periode werd er tweewekelijks gerapporteerd en waren die rapportages, die waren per dienstonderdeel apart gemaakt. Dus wij hadden toen, ik meen mij te herinneren 14 dienstonderdelen in de oude structuur. Dat was nog voor de inrichting van de topstructuur, hadden wij 14 dienstonderdelen. En die kregen van ons iedere twee weken, werden er 14 Excel-overzichten verstuurd. Dus op het moment dat je aan ons gaat vragen om nu daar een uittreksel uit te maken, dan moet ik dus vanaf 2016 van iedere twee weken 14 Excel overzichten. Nou, ga ze maar uitrekenen. Dat zijn honderden Excel overzichten waarin data uit gedestilleerd moet worden waar FSV in voorkomt.

Persoonsgegevens

Het overzicht van Persoonsgegevens is ook gebaseerd op de applicatie, op de database FSV zelf. Dat gaat IMS niet kunnen aanleveren. Dus daar zit een verrijking in van wat er in die feitelijke voorziening FSV is gedaan en wat je daarin ziet. Dat is wat anders dan wat vanuit IMS met alle moeilijkheden die daar dan, en drempels die Persoonsgegevens nu omschrijft, in zit. Als ik naga wat ze, of ze dit nog terug kan doen, dat kan ik checken. Maar dat is dus niet het hele verhaal wat vanuit IMS opgeleverd kan worden.

Persoonsgegevens

Als dat het overzicht is wat wij aangeleverd hebben gekregen vandaag waar die 30 rollen FSV in staan, als dat dat Excel overzicht is. *<er wordt verwezen naar het document '30 Rollen waarin FSV-permissie aanwezig is.xls'>*

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Oh oké. Maar het overzicht rollen waarvan FSV permissie aanwezig is *<er wordt verwezen naar het document '30 Rollen waarin FSV-permissie aanwezig is.xls'>*. En dat is een Excel overzicht. En alle informatie die daar in staat, dat is informatie die uit IMS komt. Die komt niet uit FSV.

Persoonsgegevens

Maar dan moet ik denk even checken, want de autorisatiematrix die aan het eind staat, op het vierde tabblad, die use cases, dat komt FSV.

Persoonsgegevens

Mee eens.

Persoonsgegevens

Het is een combinatierapport.

Persoonsgegevens

In het eerst tabblad staat IMS-informatie en de uitwerking op de andere tabbladen dat is informatie die niet uit IMS komt *<er wordt verwezen naar het document '30 Rollen waarin FSV-permissie aanwezig is.xls'>*.

Persoonsgegevens

Dat wilde ik even aangeven. Daar zit een verrijking in van wat feitelijk in FSV gezien kan worden.

Persoonsgegevens

Ja.

Persoonsgegevens

Persoonsgegevens

Stel dat wij vragen om die rapportages zover we dan terug kunnen, dat te gaan reconstrueren om het maar zo te zeggen, dan is dat niet hetzelfde als die bijlage die je nu ziet.

Persoonsgegevens

Nee, daar kunnen wij hoogstens de informatie die in tabblad één van de bijlage staat, zouden we eruit kunnen genereren.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Tabblad 2, die informatie kan ik ook opleveren want dat is op doelsysteem. Dat zijn de groepen die op het Windows toolsysteem staan. De rollen die er zijn en de autorisatiematrix, dat zijn FSV interne gerelateerde rollen. Als ik dat zo inschat.

Persoonsgegevens

Ik zag net Persoonsgegevens mee schudden.

Persoonsgegevens

Het klopt. Het overzicht van Persoonsgegevens was een ander overzicht dan het IMS-overzicht. Wat ik nog wel even wil aanvullen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Het is wat mij betreft nog geen afspraak.

Persoonsgegevens

Ik wou daar nog even een toelichting aan toevoegen. Sinds vorig jaar, en ik weet niet precies welke datum, zijn we gestart om wekelijks een rapportage te maken waar we, in één Excel overzicht de hele Belastingdienst hebben gecoverd. Daarvoor was het dus iedere twee weken 14 overzichten, per dienstonderdeel apart. En sinds vorig jaar hebben wij dus een bestand beschikbaar op wekelijkse basis waar alles van de hele Belastingdienst in zit. Daar

kun je dus in één bestand van zeg 50 of 55 bestanden die ik dan zou kunnen aanleveren, waar de informatie in zit of waar we die dan uit zouden kunnen filteren. Maar op het moment dat wij de periode van 2019 terug naar 2016 al die tweewekelijkse bestanden moeten gaan aanleveren, dan moet ik mensen gaan inhuren om die informatie bij elkaar te kunnen krijgen. Dus technisch gezien kan het, maar dat is heel veel handmatig werk wat daar voor verricht moet worden.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Maar als u zegt van 'ik kan een aantal cruciale data aangeven in het verleden'. Waarbij ik wat rapportage wil over wat zo dicht mogelijk bij die datum zit, dat zal de hoeveelheid werk natuurlijk ernstig reduceren.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Zullen wij afspreken dat u aangeeft welke informatiebehoefte er is. En dan zal ik u daarin een antwoord geven van wat de complexiteit is omdat op te leveren.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Wat betekent dat dan? Het is al even geleden, vijf minuten terug. En als ik dan terug kijk naar de beantwoording door de Belastingdienst, dan staat daar in, ergens aan het einde van de eerste pagina 'eind 2017 is het aanvragen van autorisatie voor FSV onder besturing van IMS gebracht'. Daar heb ik al eerder naar gerefereerd. En eigenlijk bevestigt Persoonsgegevens dat het al eerder is gedaan.

Persoonsgegevens

Exact. Dat is even wat ik wilde aanvullen waar we nooit op ingegaan zijn in dit verhaal. IMS heeft ook een ontwikkeling ondergaan, want IMS hadden we ook niet van de een op de andere dag. Wat ik begrepen heb in de gesprekken met de expert bij IMS is dat in het begin FSV wellicht aanvraagbaar was via IMS, maar niet in een rol. Maar gewoon als losse applicatie. Hij is pas opgenomen echt in een bedrijfsrol in 2017. Daarmee dus gekoppeld aan een manager die dus een medewerker een rol geeft, niet een losse autorisatie.

Persoonsgegevens

Ja. Mag ik dat iets nuanceren.

Persoonsgegevens

Graag.

Persoonsgegevens

Op dit moment is het zo het overgrote deel van de rollen die nu aangevraagd worden, die zorgen via een automatisch proces op het doelsysteem voor het toewijzen van die autorisaties. Dat noemen we 'automatische provisioning'. Daarnaast zijn er ook een aantal rollen, een aantal systemen, een aantal doelsystemen, waar IMS niet automatisch de autorisaties kan zetten, maar waarbij op basis van een roltoewijzing door een manager er een workflow wordt afgeschoten die dan richting een afdeling gaat om dan handmatig die autorisatie in de desbetreffende applicatie te zetten. Als FSV, ik denk niet, dat zou ik na moeten kijken vanaf wanneer wij dat automatisch die autorisaties kunnen zetten, maar ik kan mij goed voorstellen dat in de beginjaren van FSV er wel rollen gemaakt zijn die voor FSV toepasbaar zijn, maar dat die niet automatisch autorisaties zetten, maar dat die alleen maar een trigger zijn voor het handmatige proces om een workflow af te schieten om bij een beheerder die van die applicatie is de opdracht neer te leggen van 'je moet nu deze autorisatie gaan toekennen'. Natuurlijk hebben wij nu ook voor die situaties waarin IMS niet zelf autorisaties kan zetten, een mechanisme dat wij de werkelijkheid op het doelsysteem periodiek vergelijken met de werkelijkheid in IMS. Dat noemen we IST-SOLL vergelijkingen. Om vast te stellen dat de handmatige acties om mensen te autoriseren, dat die wel goed gegaan is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik zal dat opschrijven, ik ga dat uitzoeken en dan geef ik u antwoord of het gelukt is.

Persoonsgegevens

Dus dan zoeken we uit Persoonsgegevens

Persoonsgegevens

Ik heb opgeschreven dat ik ga uitzoeken vanaf welk moment IMS, ik doe nu even een aanname op de situatie van nu dat deze applicatie op het Windows platform is gebouwd en altijd zich heeft afgespeeld. Of heeft die in de beginjaren, is het toen op een ander platform geweest? Nee, ik denk het niet. Ik denk dat het altijd een Windows applicatie geweest is.

Persoonsgegevens

Het is een web based applicatie.

Persoonsgegevens

Dan is voor mij de taak om uit te zoeken sinds wanneer doen wij naar Windows de automatische provisioning. Als dat voor de periode ligt dat wij over FSV kunnen rapporteren, dan zit daar dus al een automatisme in. En de andere vraag die ik opgeschreven heb, is dat ik een nader verzoek krijg om rapportages op te leveren vanaf de periode september 2016, want eerder kan ik niet terug, waar we een aantal verschillende data krijgen om dan de informatie uit op te leveren.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Waarbij de periode van september 2016 tot 2019, ik weet even niet precies welke maand we dat geïntroduceerd hebben. Dus voor iedere twee weken 14 bestanden betekent en na die tijd kunnen wij op basis van één bestand per week de hele Belastingdienst destilleren.

Persoonsgegevens

Inspectie, controle en toezicht

Korte schorsing

Persoonsgegevens

Wij zaten nog even na te zoeken, ik zei mei 2018. Dat is natuurlijk heel fraai, want dat was inderdaad de ingang van de AVG. Wij hebben daar twee slagen gehad. In mei 2019 hebben wij extra controles gedaan en toen is de eerste keer FSV uit de lucht gehaald, niet mei 2018.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Je moet het wel andersom lezen. Medewerker is gekoppeld aan een rol. En de rol kent onder andere een aantal rollen binnen FSV, de applicatie rol. Dus medewerker is altijd gekoppeld aan de rol. Dus je moet echt van links naar rechts lezen. Medewerker is gekoppeld aan een bedrijfsrol. En van de bedrijfsrol ga je naar bijbehorende permissies voor de applicaties.

Persoonsgegevens

Rollen met FSV, dan is de bedrijfsrolnaam een medewerker werkt bij Grote Ondernemingen en die heeft de code 32 en daar horen verschillende dingen bij. Waaronder dat hij FSV mag raadplegen *<er wordt verwezen naar de eerste regel op het tabblad 'rollen met FSV' in het document '30 Rollen waarin FSV-permissie aanwezig is.xls'>*.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

En dan zie je dat die dan in FSV heeft die ook FSV raadplegen. Prima. Zo werkt die dus. En wat Persoonsgegevens ook uitlegde, zo'n medewerker kan nog wel meer GO-rollen hebben waar dan misschien ook nog wel FSV in zit. Dus dat kan. Je kunt als medewerker bij GO, heb je een breed takenpakket, kan je meerdere rollen hebben.

Persoonsgegevens

<er wordt verwezen naar het tabblad 'rollen met FSV' in het document '30 Rollen waarin FSV-permissie aanwezig is.xls'> Ik denk dat dit Excel overzicht, het eerste tabblad van het Excel overzicht geeft in de linker kolom, geeft het een aantal rollen weer en daar staat in de tweede kolom staat de logische omschrijving van die rol. De eerste is alleen maar een code. En in kolom C staat hoeveel mensen er aan zaten op dat moment. Niet wie, maar het aantal users. En in kolom drie welke FSV onderdeel in die rol zit. Maar dat kan dus best zijn dat aan die rol D, VO32 er meer permissies zaten, dan in kolom D is weergegeven. Maar dat kunnen dan permissies zijn voor andere applicaties die in dit kader niet relevant zijn.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Als er gezocht is op permissies, dat lijkt mij logisch, op FSV-permissies. Dan is dat het zoek item geweest voor dit overzicht. En wij hebben gezegd welke permissies zitten aan welke rol. Zo is dit overzicht tot stand gekomen. Het is niet zo dat er dan meer rollen zijn die hier niet benoemd zijn waar ook een permissie met FSV in zit. Want dat werd net ook even gesuggereerd. Nee, dit zijn alle rollen waar permissies in zitten die met FSV te maken hebben. Er zijn niet andere rollen waar ook FSV dingen in kunnen zitten. Op dat moment dat de rapportage is gemaakt.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. De manager ziet dus wat in kolom A en B staat *<er wordt verwezen naar het tabblad 'rollen met FSV' in het document '30 Rollen waarin FSV-permissie aanwezig is.xls'>*, ziet hij in zijn IMS-omgeving. Zijn web portaal. Daar kan hij zoeken op die rol en daar kan hij daar zijn medewerker aan koppelen. Zo connect hij die user aan een rol en dan gaat het hele proces werken dat de autorisaties die in die permissie zitten en alle permissies die in die rol zitten, die autorisaties worden dan aan die medewerker uitgereikt. Dan wel via een automatische mechanisme, dan wel via een handmatig mechanisme. Het is zelfs denkbaar dat een deel van de permissies die in zo'n rol zitten automatisch gaan en dat andere permissies eerst nog een workflow afschieten om een handmatig proces in te gaan om dan uiteindelijk die autorisatie te krijgen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is een goede vraag.

Persoonsgegevens

Dit zijn twee vragen eigenlijk en die hebben ook een beantwoording in de tijd verschillend. En ik zit even te twijfelen of ik dan Persoonsgegevens of Persoonsgegevens misschien eerst het woord moet geven. Misschien Persoonsgegevens eerst even in algemene zin. Want hier gaat het dus eigenlijk om wat deed die beheerder die dan feitelijk die toegang geeft tot die applicatie. Dus die toekenning doet en de controle daarop.

Persoonsgegevens

Ik hoor hem iets anders.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Dat is eigenlijk de vraag die Persoonsgegevens zou moeten kunnen beantwoorden, Persoonsgegevens eigenlijk ook als afdelingshoofd of als teammanager. Want dat is precies hun taak. Dus het lijkt mij bij uitstek een vraag voor onze managers.

Persoonsgegevens

Dan geef ik het eerst aan Persoonsgegevens

Persoonsgegevens

Ik kan er eigenlijk heel weinig over zeggen, want ik ben nooit afdelingshoofd of manager geweest van FSV.

Persoonsgegevens

Oké, dan ga ik terug in mijn geheugen.

Persoonsgegevens

Even Persoonsgegevens om te helpen Persoonsgegevens gaf net al aan dat er wel degelijk overzichten periodiek gemaakt worden, die ook wel bij managers terecht komen, om te checken. Want ik kijk naar mijn medewerkers, ik kan niet in FSV. Niemand van mijn medewerkers kan dat omdat wij daar niets met het proces te maken hebben. Als het gaat om de uitvoering ervan. Maar ik krijg wel degelijk IC checks dat ze zeggen 'jouw medewerker heeft nog de rol inspecteur, dat kan niet want hij werkt, klopt dat nog, doe daar iets aan'. Maar dan netter verwoord. Dus die checks die krijg ik. En ik voer het dan uit. Dan geldt bijvoorbeeld ook voor samenwerkingsgebieden. Dat wordt ook gecheckt. 'Gij zult schonen' van klopt het allemaal nog wel.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is inderdaad vraag twee. Dat ziet veel meer op de autorisatie matrix. Dat is eigenlijk het model wat hier achter zit, waarin er bepaald wordt welke permissies heb je nou nodig binnen een bepaalde bedrijfsrol. Dat ligt niet bij die manager. Dat is wel de verantwoordelijkheid van een directeur op zijn eigen bedrijfsonderdeel. En dan spreek ik alleen voor de situatie 2018 en later want hoe het voor die tijd was, ik heb werkelijk geen idee hoe toen die autorisatiematrix tot stand kwam. Maar sinds 2018 is een directeur verantwoordelijk voor zijn eigen autorisatiematrix. Daar beschrijft hij dus welke applicaties hij nodig heeft, in zijn totaliteit, binnen zijn directie, om zijn mensen het werk te kunnen laten doen. Daar is een autorisatiematrix beheerder die dus die inhoudelijke afstemming doet, samen met het team Persoonsgegevens bij FM&I, om die autorisatie matrix van de IMS in te lezen zodat de manager uiteindelijk de rollen kan toekennen aan zijn medewerker. Dus manager ziet niet wat er aan applicaties in die rol zit, dat is voorbehouden aan de autorisatiebeheerder. En hoe dat precies zit, dat kan Persoonsgegevens als het goed is toelichten.

Persoonsgegevens

Ja. Daar kan ik wel een korte toelichting op geven. Je moet je eigenlijk voorstellen dat wat in kolom D staat, die permissies, dat is eigenlijk het niveau waarop je autorisaties zou willen uitreiken. Dat is het meest sprekende. Dat zijn de individuele functierollen in een applicatie. Bijvoorbeeld FSV behandelaar. En die permissies of permissieniveau worden ook de autorisatie matrix samengesteld van: 'mijn medewerker die moet behandelaar FSV zijn, die moet raadplegen A, B, C en muteren X, Y, Z'. En daar komt dan een samenstel van permissies uit. En op basis van die permissie worden door mijn collega's van het team rollenbeheer, die een soort consultancy rol vervullen naar de verschillende dienstonderdelen toe, wordt op basis van de autorisatiematrix waar de dienstonderdeel van is, gaan mijn collega's samen met de contactpersoon van die autorisatiematrix, voor dat dienstonderdeel, die permissies logisch groeperen tot één of meerdere rollen. De rollen die in kolom A en B staan, die zijn conform de conventies die wij in het LTB-proces hebben gesteld, zijn die gemaakt. Daarbij hebben onze collega's die technisch gemaakt. Die hebben dat in afstemming gedaan met de gemandateerde vanuit ieder dienstonderdeel die op basis van de autorisatie matrix, die binnen dat teamonderdeel is vastgesteld, de bevoegdheid heeft om aan ons te vertellen van 'nu moet je FSV behandelaar voor die verschillende teams in rollen beschikbaar stellen'.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Een autorisatiematrix is een on going proces. Zo'n autorisatiematrix die wordt gemaakt, dan wordt hij ingericht. Op het moment dat er wijzigingen komen, er komt een nieuwe applicatie of er zijn veranderingen nodig in de applicatiematrix, dan wordt dat via een regulier proces door het team, mijn collega's van rollenbeheer, met de vertegenwoordigers van de dienstonderdelen afgestemd. Dus die autorisatie matrix die wordt eigenlijk continue onderhouden, op basis van de wijzigingen die er voortkomen uit bijvoorbeeld de voortbrenging van nieuwe applicaties of wijzigingen die er doorgevoerd worden in een applicatie.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Dat is wel interessant. Daar gelden inderdaad, daar zijn de dienstonderdelen hebben daar een bepaalde autonomie in op basis van de aan hun aangeleverd BI-rapportages, daar interne beheersingsmaatregelen op te nemen. Maar aan de andere kant, als je in een team zit en jouw medewerker heeft een rol en die rol is niet aan verandering onderhevig en je hebt jouw medewerker een rol gegeven in IMS, dan is er ook weinig aanleiding om aan te nemen dat die rol niet meer voldoet. Een medewerker moet daar natuurlijk, een manager moet daarover in gesprek zijn met zijn medewerker, dat ze daar periodiek eens naar kijken. Maar dan nog geldt van 'als ik zie ik zit aan die rol en die rol hoort bij mijn team en die hoort al drie jaar bij mijn team', dan zijn ze gauw klaar met het gesprek, want als die rol wijzigt, dan wordt die manager daarvan op de hoogte gesteld. Dat er een wijziging is aangebracht in de rol waar zijn medewerkers aan zitten. Dus die informatie kan hij dan, dan zou hij eventueel kunnen besluiten van 'ik haal mijn medewerkers van die rol af'. Maar andersom is het zo, die wijzigingen die in die rol gedaan worden, die komen in samenspraak met de gemandateerde vanuit een dienstonderdeel tot stand. Dat is, wat Persoonsgegevens net al zei, dat is niet altijd de manager die dat bepaalt. Meestal niet zelfs. Die autorisatie matrix die komt via een andere weg tot stand.

Wat ik daar nog wel aan toe zou willen voegen, misschien, nog één kort vermelding. Als een medewerker nou gaat verplaatsen naar een ander team of een ander onderdeel, dan voorziet IMS wel in een mechanisme dat de bestaande rollen automatisch worden verwijderd.

Persoonsgegevens

Ik zou daar nog iets aan willen toevoegen als dat mag. De vraag is ook een beetje van 'hoe weet nou dat die autorisaties of de applicatie nog steeds horen bij die rol?'. Dat is eigenlijk de andere kant van de sport. Die beoordeling daar komen we zelden of nooit aan toe want dan komt er weer een reorganisatie en dan moet je je autorisatie matrix opnieuw opstellen. Dan wordt ook opnieuw het hele circus doorlopen. Dan is eerst dat je gaat zorgen dat medewerkers hun werk kunnen blijven doen. Dus wij komen eigenlijk nooit in een beheersituatie dat wij die autorisatie matrix, in een soort van stabiele versie hebben die wij dus periodiek kunnen toetsen van klopt het nog bij het werk. De wijzigingen van de organisatie gaan sneller dan het periodiek toetsen van: klopt deze autorisatie nog bij de medewerker, bij het type werkzaamheden.

Persoonsgegevens

Ik kan u niet zo goed verstaan, maar misschien kunnen we het wel samenvatten.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Exact. De dagelijkse mutaties, als het gaat om nieuwe applicaties en er verdwijnen applicaties en wijzigende applicaties, samen met organisatiewijzigingen maakt dat de organisatie matrix constant in beweging is. Dat er niet echt een moment is dat je kan zeggen 'dan gaan we eens even kijken of nog steeds de applicaties nu echt horen bij dat type werk'. Dan moet je eigenlijk het proces beoordelen. Je gaat niet een losse autorisatie beoordelen, je gaat het proces beoordelen van: er wordt gezegd van op de manier waarop we het zouden moeten doen. Dan kom je tot welke applicatie hebben we dan nodig voor het proces en dan kom je tot welke medewerkers moeten dat uitvoeren. Dat is niet een losse activiteit die je zo ergens op een vrijdagmiddag doet. Je moet dan het hele proces beoordelen. Je kan niet zeggen als manager 'doe mij maar applicatie meer of minder om mijn werk te kunnen doen', want dat is een beheersproces.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is een aspect wat nog niet ter sprake gekomen is. Als je zo'n rollenmodel maakt, dan probeer je dat zo generiek mogelijk te maken. Je stopt soms meer applicaties in een rol, dan een medewerker daadwerkelijk nodig heeft. Je gaat niet voor iedereen kijken of ze dagelijks Word nodig hebben. Word zit in een algemene rol die iedereen heeft. Zo is dat ook waarschijnlijk gegaan met FSV. FSV was een soort van lokaal ontwikkelde applicatie opgenomen als een soort van basisvoorziening die iemand kan gebruiken voor het raadplegen in zijn werk. Of hij het iedere dag nodig heeft, onbekend. Wij stoppen het in een basisprofiel voor een Grote Onderneming raadpleger. Of hij het daadwerkelijk nodig had, geen idee. Dat zat gewoon in dat profiel. Dat je geautoriseerd bent voor FSV, wil niet automatisch zeggen dat je het ook iedere dag gebruikt. Wat er gedaan is in die actie op 24 mei, is gekeken van wie gebruikt er nu daadwerkelijk van al die mensen die in hun rol, in theorie toegang hebben tot FSV, wie heeft het nu echt nodig. Zo zijn ze teruggegaan van 5.000 naar 1.000.

Persoonsgegevens

Daar wil ik graag nog even op toespitsen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Er zitten in een rol soms meer applicaties dan een medewerker daadwerkelijk iedere dag nodig heeft. Soms heeft hij het één keer in het jaar nodig, misschien wel nooit. Als ik in mijn eigen rolmodel kijk, zitten er ook applicaties in, niet op primair proces maar in bedrijfsvoeringen, bijvoorbeeld mindmapping. Ik maak nooit een mindmap, maar hij zit wel in mijn rol beleidsmedewerker omdat de gemiddelde beleidsmedewerker blijkbaar ook wel eens een keer een mindmap moet kunnen maken. Dus in de rollenmodellen zoals je ziet, zie je de autorisatie die een medewerker kan hebben of heeft, maar dat zijn niet de applicaties die hij

ook iedere dag hoeft te gebruiken. Dat is precies wat er met FSV gebeurd is in mei. Wij hebben gekeken van wie gebruikt nu daadwerkelijk FSV en daar zijn de autorisaties voor behouden en andere mensen hebben wij uit FSV geknipt. Die mogen niet meer in FSV.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

De 'we' is nou even in dit geval de heer Persoonsgegevens geweest, die helaas niet aanwezig kon zijn. Dat is ook de actie die ook in de Kamerbrief beschreven is. Dat hebben we ook in de tijdlijn op die manier opgeschreven. Dat is een actie die onder regie van MKB toen uitgevoerd is. Ik weet niet of Persoonsgegevens daar nog relevante, Ik denk het niet, dat was voor jouw tijd. Dat heeft MKB op dat moment uitgevoerd als de business owner. Dus daadwerkelijk gekeken wie heeft nog echt FSV nodig voor zijn werk.

Persoonsgegevens

Dit refereert aan de actie waarvan wij net zeiden dat was 24 mei 2019.

Persoonsgegevens

En de aanleiding was daarbij, dat heb ik net uitgelegd, dat er nog AVG checks liepen naar aanleiding van een export functies en aantallen users. Daar op basis van is toen gezegd 'hier moet opnieuw naar gekeken worden'. Toen hebben MKB en IV hier die actie op gehad.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat weet ik niet. Ik heb geen idee wat de directies inhoudelijk doen op hun organisaties.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Persoonsgegevens kan het antwoord geven.

Persoonsgegevens

Er is natuurlijk ook een proces dat de eigenaar van een applicatie, van al die 1.000 applicaties die wij gebruiken, dat die wel regelmatig gaan monitoren op basis van de rapportages die hij heeft, van wie zitten er allemaal aan mijn applicatie en hoe vaak maken die mensen daarvan gebruik. Dat wordt niet voor alle applicaties heel specifiek gedaan, maar ik weet dat er ook vanuit die analyses beperkingen aan ons doorgegeven worden van 'je moet die dingen uit die rollen gaan halen'. Want stel nou dat er een permissie aan een rol toegevoegd is en dat vastgesteld is dat er maar één medewerker van het team die in die rol heel periodiek die rechten gebruikt, dan wordt zo'n permissie uit een generieke rol gehaald en dan wordt daarvan gezegd 'dan maken wij daar een bijzondere taak van'. En die wordt dan aan die ene medewerker beschikbaar gesteld. Dus via dat proces leidt de verfijning die

op initiatief van de eigenaar verantwoordelijke van de applicatie of het proces waar de applicatie ondersteunend aan is tot een inperking van het aantal users wat toegang heeft tot die resources.

Korte schorsing omdat mevrouw Persoonsgegevens s weggevallen

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat was een toevoeging die ik gegeven heb. Een eigenaar van een applicatie die monitort op basis van de rapportages die hij krijgt, monitort hij ook van wie zitten er allemaal aan mijn applicatie; wie maken daar gebruik van. En die krijgen ook rapportages via andere wegen van hoe vaak wordt er ingelogd door personen. Dat kan een aanleiding zijn dat een eigenaar zegt van, die permissie voor FSV die in een rol zit waar het hele team er gebruik van maakt, zou mogen maken en dat hij dan vaststelt dat er maar een enkeling van het team daar gebruik van maakt, dat hij dan zegt van 'dan halen we die permissie uit de teamrol en dan maken we daar dan zogenaamd een bijzondere taak van die wij aan twee mensen uitreiken'. Daardoor kan het aantal users wat aan een permissie gekoppeld zit, ook minder worden. Dat is wat ik nog wilde toevoegen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Daar kan ik geen antwoord op geven. Want in het kader van de AVG hebben wij verwerkingsafspraken met de dienstonderdelen aan wie wij op persoonsbasis onze rapportages uitreiken. Wat de dienstonderdelen met die rapportages doen, dat kan ik dus niet beoordelen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

De eigenaren van FSV die zitten ook bij een dienstonderdeel.

Maar het gebeurt ook dat eigenaren bij ons ad hoc rapportages opvragen om inzicht te krijgen in specifieke dingen die voor zijn applicatie van toepassing zijn. Want je kan je voorstellen dat als een eigenaar van FSV informatie zou willen hebben en ik moet hem dan een bestand aanleveren waar informatie over nog 500 andere applicaties in zit, dat dat niet gewenst is. Dus daar hebben wij dan een mechanisme voor ad hoc rapportages voor. Maar die worden niet bewaard. Die worden uitgereikt en die worden dan op ad hoc basis gebruikt. Dus daar heb ik geen inzicht in en zeker niet in een lange periode terug.

Persoonsgegevens

Ik denk dat wij zonder Persoonsgegevens die niet bij dit gesprek aanwezig is, niet kunnen vaststellen of er periodiek zo controle is geweest. Zeg ik het zo goed Persoonsgegevens

Persoonsgegevens

Dat denk ik ook.

Persoonsgegevens

Dit moet terug in ieder geval naar de eigenaar, wat dan MKB is, en daarnaast zijn er meerdere gebruikers, gebruikende uitvoerders directies. Voor die vragen is het dan, die vraag moet naar MKB, maar die moet dan ook naar P en andere gebruikersgroepen die wij dan hebben.

Persoonsgegevens

En als ik even de vrijheid mag nemen, ik denk dat jullie dan aan ons gaan vragen van 'willen jullie uitzoeken of dat soort rapportages er zijn geweest en of die activiteiten zijn geweest'. Ik denk dat dat voor ons heel erg moeilijk is terug te halen. Dat heeft te maken met dat de betreffende collega's soms niet meer in dienst zijn, heeft ook te maken met reorganisaties. Dus wij zullen het zeker wel vragen aan Persoonsgegevens maar als hij het niet goed weet, dan hebben wij eigenlijk niet veel andere opties om het na te gaan of het gebeurd is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, dat is MKB.

Persoonsgegevens

Vanaf 1 januari 2018 topstructuur.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is dus Persoonsgegevens

Persoonsgegevens

Dat is wat Persoonsgegevens aangeeft. Dat is Persoonsgegevens die is hier langere tijd bij betrokken geweest en die kan ook met zijn MT hier het gesprek over voeren als dat nodig is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Hij was toen de eigenaar ja.

Persoonsgegevens

Wij hebben geen eigenaar in naamspersoon. Het MT MKB is eigenaar.

De heer Persoonsgegevens
Hij was de gedelegeerd business owner en als zodanig acteerde hij als eigenaar.

Persoonsgegevens
Dus hier maken wij een knip in de periode. Wij hebben net toegelicht dat op een gegeven moment het eigenaarschap overgegaan is naar de keten Generiek en Kantoor Toezicht. Ik zeg de naam niet helemaal goed en daarvoor was dus het eigenaarschap bij MKB. En daarvan is ons aanspreekpunt Persoonsgegevens Hij kan eventueel met zijn MT nagaan of dat voor die tijd ook gebeurde. Maar eigenlijk neem ik nu al een voorschot op dat antwoord. Ik denk dat dat niet meer beschikbaar is. Dus we kunnen het denk ik niet goed bevestigen of dat gebeurd is. Of aantonen, laat ik het zo zeggen.

Persoonsgegevens
Even als aanvulling. FSV, TSV en alles wat daarbij hoort zit in het domein GKT. Dat klopt. Daar ben ik dan gedelegeerd van vanuit die keten voorzitter. Maar het is niet zo dat de keten ten aanzien van autorisaties verantwoordelijkheid overneemt omdat dat bij de lijn hoort. Ik kan niet verantwoordelijk zijn voor medewerkers, die vallen onder een directie MKB, P enzovoort. Dat zit in de lijn geborgd.

Persoonsgegevens
Inspectie, controle en toezicht

Persoonsgegevens
Inspectie, controle en toezicht

Persoonsgegevens
Daar zal ik denk ik hetzelfde antwoord geven. Wij zullen dat navragen bij Persoonsgegevens maar mijn verwachting is dat ik dat niet aantoonbaar terug kan halen.

Persoonsgegevens
Inspectie, controle en toezicht

Persoonsgegevens
Niet over die, je vraagt nu naar een periode. Ik kan dat wel, nu hebben wij dit soort processen wel vastgelegd. Maar voor 2018 is dit lastig te reproduceren.

Persoonsgegevens
Inspectie, controle en toezicht

Persoonsgegevens

Dat zijn denk ik nu de afspraken die wij hebben met LTB over het periodiek laten rapporteren en die processen.

Persoonsgegevens

Het rapporteren naar de bedrijfsonderdelen, dat antwoord weer terug hebben, dat heb wij nog niet ingericht.

Persoonsgegevens

Sorry, ik versta u niet goed.

Persoonsgegevens

Wat wij ingericht hebben nu is de terugkoppeling naar de eigenaren van de overzichten zoals de heer Persoonsgegevens aangaf. Wij hebben nog niet ingericht de terugkoppeling wat de Persoonsgegevens daar daadwerkelijk mee gedaan hebben.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik denk dat Persoonsgegevens moeten dan aangeven hoe het nu ingeregeld is en dat wat we niet doen, moeten we dan ook gewoon melden dat we dat niet doen.

Persoonsgegevens

Maar dat is niet als een generiek proces ingericht. Daar ligt een autonome bevoegdheid bij de verschillende dienstonderdelen om daar invulling aan te geven op basis van de beheersmaatregelen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, helder.

Persoonsgegevens

Ik wil eigenlijk geen extra werk hebben. Maar wat ik zal doen, is dat ik nog ga checken met Persoonsgegevens maar ook bij mij in de keten of ik in ieder geval in het systeem kan terughalen, maar dat is dan echt FSV-gebaseerd en niet IMS-gebaseerd. Of wij dat kunnen zien dat er eerder dit soort sessies geweest van opschonen. Dus dat ga ik, voor zover ik dat kan achterhalen, neem ik die nog mee om te checken.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is dan wat je in het systeem kunt.

Persoonsgegevens

Wij vanuit IMS kunnen alleen maar de informatie opleveren wat ik straks heb gezegd, wanneer hebben wij welke rapportages uitgeleverd en wat er vervolgens aan acties intern bij een dienstonderdeel op die rapportages zijn uitgezet, hebben wij geen zicht op.

Persoonsgegevens

Dat hebben we afgesproken dat we die vraag meenemen naar MKB.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is de actie die bij mij ligt om uit te zoeken vanaf welk moment IMS-autorisaties automatisch provisioned naar de doelsystemen waar FSV op draait.

Persoonsgegevens

Of dat er nog handmatige, dat is wat we dan zouden willen weten, of er nog een handmatig proces tussen zit of dat dat proces al in de tijd ook al geautomatiseerd was of dat het een semi-automatisch proces was met een gedeeltelijk handmatig deel erin.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Nee. Wat ik ga doen, want er werd net gevraagd over, zijn er nou eerder van die checks gedaan naar aanleiding van 5.000 naar 1.000? Zijn er al eerder van dit soort checks geweest? En ik ga checken of ik dat in het systeem terug zou kunnen vinden. Of dat inderdaad zo is. Ik heb daar niet heel veel verwachtingen op, maar het is wel een check die wij in het systeem nog kunnen doen.

Volgens mij, ik heb in ieder geval opgeschreven, dat er nog was de procedures zoals die nu zijn na 2018 die worden opgeleverd. Dat is een actie voor IV&D en [Persoonsgegevens]. En dat we nog gaan checken bij [Persoonsgegevens] bij MKB, hoe de checks daar verlopen zijn naar aanleiding van rapportages die opgeleverd worden vanuit IMS.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Welke procedures refereer je dan aan Persoonsgegevens

Persoonsgegevens

De control procedure eigenlijk.

Persoonsgegevens

Welke interne controle mechanisme hebben wij. Dat is de vraag dacht ik.

Persoonsgegevens

Daar kan een deel van landelijk zijn, voor de hele Belastingdienst. Maar het grootste gedeelte ligt daar op organisatie onderdeel niveau.

Persoonsgegevens

Even voor de zekerheid. Juist vanwege het feit dat een heel groot deel organisatie afhankelijk is, zijn jullie alleen geïnteresseerd in die organisatieonderdelen die FSV gebruikten of generiek Belastingdienst breed alle 23 directies?

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Oké. Dus Particulieren, MKB en CAP.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

En Toeslagen, ja. Vier directies.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Nee, GO gebruikt FSV niet.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat staat ook in het KPMG rapport.

Persoonsgegevens

Niet meer.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Daar had de FIOD ook toegang.

Persoonsgegevens

Heel beperkt. FIOD heeft ook toegang gehad. Maar ook heel beperkt. Ik denk iets van drie of zo. Dat doe ik even uit mijn hoofd.

Persoonsgegevens

Ja. Voor externe inzageverzoeken, niet voor reguliere projecten van fraudesignalen.

Persoonsgegevens

Dat is de check aan de AP: of zij het volledig willen of alleen de grootgebruikers.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, de onderdelen die toegang hadden tot FSV. In die autorisatie matrix tabblad één.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Klopt. En tijdens de sessie heb ik het al doorgestuurd. Maar dat klopt. De tijdlijn van dat FSV al eerder aansloot op IMS.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik heb nog even een nabrander. Ik heb net even gekeken wat mevrouw Persoonsgegevens gestuurd heeft. Daar moet ik intern nog even over babbelen of dat wij het over hetzelfde hebben. Dit is precies het onderdeel wat even niet in het verhaal naar voren kwam. Ik zei al IMS is enig moment begonnen, in 2012 denk ik. Ik kijk even naar Persoonsgegevens Misschien 2011. Toen hadden we natuurlijk niet op dag één alle applicaties op de juiste manier in alle mogelijke rollenmodellen zitten. Dat is een groeimodel geweest. Wat ik nu even zie in de mail Persoonsgegevens die jij me opstuurt, is dat daar de vijf losse permissies die je in FSV kan krijgen, in IMS opgenomen zijn. Daarmee zit het nog niet automatisch ook de rollenmodel. Maar je kon wel IMS gebruiken om FSV te bestellen als los product.

Persoonsgegevens

Volgens mij zit, we moeten nu niet de discussie denk ik opnieuw voeren. Wij kunnen het daar over hebben en volgens mij heeft Persoonsgegevens ook aangegeven dat hij nog de check doet op wat automatisch zat of wat nog via mail ging of via workflow moet ik zeggen.

Persoonsgegevens

Ja, dat klopt.

Persoonsgegevens

Laten wij het oppakken en een duidelijk antwoord opschrijven voor de AP.

Persoonsgegevens

En wat ik in een eerder bericht aan de AP gestuurd heb, is wanneer FSV daadwerkelijk echt in een rolmodel zat, gekoppeld aan andere applicaties. Dus niet meer al los product maar als onderdeel van.

Persoonsgegevens

Wij moeten het goed uitwerken, want anders is het onbegrijpelijk denk ik.

Persoonsgegevens

Exact. Dus we moeten even intern nog over schakelen wat we daarover terugkoppelen.

Persoonsgegevens

Prima. Doen we.

Persoonsgegevens

Heeft het jullie geholpen en begrijpen jullie waarom het voor ons lastig was om daar duidelijk antwoord op te geven met de vraagstelling die wij hadden?

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Oké. Dankjewel.

Ik wilde nog één opmerking maken voor de zekerheid. Volgens mij ligt die heel erg voor de hand, maar jullie openden deze vergadering eigenlijk met naar aanleiding van de GEB. Ik wil

wel vastgesteld hebben dat het gaat om een concept GEB. Dus dat die eigenlijk nooit echt verder gebracht is in de evaluatie, in de besluitvorming. Dat op het moment dat die bij Persoonsgegevens bekend werd als zijnde privacy officer om daarnaar te kijken, dat er toen ook direct actie is genomen. Dat we het hier niet over een vastgestelde GEB hebben, maar echt over een concept GEB die nog in de organisatie niet de eindstatus heeft gehad. Het maakt het niet minder erg, maar dat het wel een concept GEB is.

Persoonsgegevens

Oké. Het is goed dat u dat toevoegt.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Mooi. Daar ging ik eigenlijk ook wel vanuit. Maar ik hoorde hem niet terug. Dus vandaar dat ik hem nog eventjes daarmee terughaal.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dan kijk ik denk ik even naar Persoonsgegevens wat voor hem het beste haalbaar is.

Persoonsgegevens

Die datum kan ik pas afgeven als ik de vraag van u ontvangen hebt. Dat bepaalt de complexiteit en de doorlooptijd van de acties die ik moet uitzetten. Dat moet ik ook laten uitzetten bij collega's. Zodra ik de vraag beschikbaar heb, zal ik daar op een korte termijn daarna een indicatie afgeven wanneer wij dat kunnen opleveren. Maar ik weet niet of mijn acties in alle vragen die gesteld zijn, de langste doorlooptijd heeft.

Persoonsgegevens

Ik stel voor dat wij dan na deze vergadering, als u weet welke data het zijn, dat we Persoonsgegevens vragen wat een redelijke termijn is. Dat ik die aan u terugkoppel of Persoonsgegevens koppelt die dan aan u terug. Dan horen wij of dat, dan kunnen wij daar nog wel even over afstemmen of dat voor u redelijk is en of dat oké is. Oké?

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Het één hoeft niet per se van het andere af te hangen.

Persoonsgegevens

Oké. Hartelijk dank iedereen voor de tijd en de moeite.

Persoonsgegevens

Ja, jullie ook heel erg bedankt voor de extra tijd die wij hebben gekregen. Dankjewel.

Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: maandag 4 januari 2021 13:44
Aan: Persoonsgegevens
Onderwerp: z2020-04615 - reactie op verklaringen van 2 december 2020 en aanvullende informatie

Geachte mevrouw Persoonsgegevens

Ik reactie op uw bericht van 15 december 2020 over de uitwerking van de verklaringen van 2 december 2020 bericht ik u als volgt.

Reactie op de verklaringen:

-dhr. Persoonsgegevens : geen opmerkingen
-mw. Persoonsgegevens : geen opmerkingen
-mw. Persoonsgegevens : geen opmerkingen
Persoonsgegevens : geen opmerkingen
Persoonsgegevens opmerkingen in bestand en aangeboden via bestandenpostbus (IOS)
-dhr. Persoonsgegevens : opmerkingen in bestand en aangeboden via bestandenpostbus (MS)

Aanvullende informatie over de wijze van opname van de rollen van FSV in IMS vóór 2017; informatie van Persoonsgegevens Persoonsgegevens

Er zijn drie documenten aangeboden via de bestandenpostbus.

-Handreiking voor de manager uit 2013 voor het toekennen van autorisaties (document "2013-08-02 Autorisaties dagboek FSV (Handreiking voor M2).pdf");
-Handreiking voor de medewerker uit 2013 voor het autoriseren (document "2013-11-07 Handreiking Autorisaties Dagboek FSV.pdf").
-In beide handreikingen is sprake van een spreadsheet met detailinfo. Dat betreft bijgaande spreadsheet (document "2013-08-07 IMS profielen.pdf")

Aanvullende informatie van dhr. Persoonsgegevens

twoord op de vraag m.b.t. de datum waarop we de rollen op de Active Directory automatisch provisionen is als ɹgt.
Sinds november 2014 worden door IMS de FSV-autorisaties via een automatische koppeling (met de Windows Active Directory) gezet.
Dus in de periode waarover we vanuit IMS hebben gerapporteerd over FSV was deze koppeling operationeel.

Contact met ADR over documenten

In reactie op de vraag of de ADR beschikt over een lijst/overzicht met documenten die de ADR gebruikt heeft de ADR als volgt gereageerd.

[...] *Het dossier Basispositie AVG van de BD is al gearchiveerd (2018-FIN-054), dus ik kan niet eenvoudig in het dossier.*
Bijgevoegd is het eindrapport, maar daar staat niet iets in over autorisaties.
Dus op dit moment kan ik je geen aanvullende documentatie aanleveren.
Ik denk ook niet dat er informatie over autorisaties in het dossier is opgenomen. [...]

De ADR heeft op 18 december 2020 een kopie van het eindrapport gestuurd: 'Basispositie AVG van de BD' van 8 juni 2018 (kenmerk 2018-0000107347).
Het door de ADR genoemde eindrapport is aangeboden via bestandenpostbus.

Daarnaast stuur ik u de berichten die ik van de ADR ontvangen heb via de bestandenpostbus.

AANVULLING op antwoord: Waarom heeft de Belastingdienst de bedoelde rapportages van MKB, Toeslagen, PDB, GO, DF&A en FIOD tot op heden niet aangeleverd aan de AP?

In aanvulling op het bericht van 11 december 2020 en in reactie op hetgeen ik tijdens het telefoongesprek van 15 december 2020 (onder voorbehoud) desgevraagd heb aangegeven, hebben de directies MKB, P, GO, DF&A en Toeslagen het schonen van de autorisaties gemeenschappelijk uitgevoerd. Uit het eerder aan de AP opgeleverde document "01 Eindrapport actuele Soll.pdf" blijkt dat door F&MI in samenwerking met de directies invulling gegeven is aan de opdracht om te schonen. Met dat document is dan ook de verantwoording over de opdracht tot het actualiseren van autorisaties opgeleverd.

Ten aanzien van de zin "Een rapportage van een directeur over de actualiteit van autorisaties per 1 oktober 2018 zoals gevraagd in de opdracht van de directeur IV&D, is niet aangetroffen bij de Belastingdienst." informeer ik u als volgt.
De directeuren moesten naar een einddoel werken ('verplichting naar resultaat'), zij mochten zelf bepalen op welke wijze.
Er is geen andere verslaglegging vóór 1 oktober 2018, dan genoemd eindrapport.
Het eindrapport is opgeleverd aan het DTBD.

Verder is de implementatie van de AVG is bij de Belastingdienst in twee etappes uitgevoerd: een zogenaamde basispositie per mei 2018 en een vervolgtraject tot en met mei 2019. Een deel van de acties die na 25 mei 2018 nog niet afgerond waren, zijn opgenomen in een document "180716 notitie DT beleidslijnen en acties AVG geconsolideerd.pdf" (vastgesteld in DT juni 2018 als onderdeel van eindrapport basispositie AVG).
In dat document is de volgende actie benoemd:
Elk dienstonderdeel toetst voor 1 oktober 2018 actief de actualiteit van bestaande autorisaties en neemt maatregelen om niet actuele autorisaties in te trekken.

Persoonsgegevens heeft destijds in een separaat bericht nogmaals aandacht gevraagd voor deze actie; dit bericht wordt t.z.t. nagezonden.
Met het meermaals genoemde eindrapport is de verantwoording over de opdracht tot het actualiseren van autorisaties opgeleverd.

De FIOD heeft als volgt gereageerd op de vraag waarom de FIOD niet meegedaan heeft aan de centrale actie om de autorisaties op orde te brengen.

Binnen de FIOD hangt de aandacht voor het autorisatieproces niet zozeer samen met de AVG als wel met de Wet politiegegevens (Wpg). Het proces van autoriseren én de controle hierop alsmede de controle op de toegekende autorisaties maakt integraal onderdeel de interne controle, kan worden betrokken in de interne audit én wordt betrokken in de privacy audit.
Wij benadrukken dat alle autorisaties worden aangevraagd en toegekend in IMS. De FIOD kent geen autorisaties die, direct na aanvraag in IMS, geautomatiseerd worden toegekend. Elke aanvraag wordt voorgelegd aan een afzonderlijk team van goedkeurders. Om een zorgvuldige afweging te kunnen maken wordt altijd gekeken naar de reeds toegekende autorisaties (i.v.m. mogelijk conflicterende autorisaties).
Vanuit het interne controleprogramma van de FIOD wordt frequent en vanuit meerde invalshoeken gekeken of autorisaties terecht zijn toegekend. Dit zowel steekproefsgewijs op user-niveau, vanuit de applicaties en het in- uit- en doorstroomproces van de medewerkers. En maakt, zoals hiervoor ook reeds aangegeven, het 'torisatieproces én de autorisatie sec ook integraal onderdeel uit van de (Wpg) privacy audit.

ık vertrouw erop u hiermee van dienst te zijn geweest.

Met vriendelijke groet,

Persoonsgegevens

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

Persoonsgegevens

Bylage 1

Autorisaties dagboek Fraude Signalering Voorziening

De applicatie "Dagboek F.S.V." is bestemd voor de registratie van fraude signalen welke voorheen in dagboek PIT (oud) werden geregistreerd.

Primair is deze applicatie ontwikkeld voor de registratie van alle soorten van signalen betreffende de zogenaamde "systeemfraude". Hiermee wordt hoofdzakelijk bedoeld het min of meer opzettelijk misbruiken van fiscale regelingen. Dit kan zijn in de inkomstenbelasting, loonbelasting, omzetbelasting, maar ook voor de verschillende Toeslagen (huur, zorg, kinderopvang) enzovoorts.

Ook kan deze applicatie gebruikt worden voor de registratie van tips/kliks/signalen, projecten (per segment, regionaal, plaatselijk) in het Subject Gerichte Toezicht (S.G.T.). Voorts de registratie van bijzondere verzoeken om informatie. Je moet hierbij denken aan verzoeken in het kader van strafrechtelijke onderzoeken (bijv. zogenaamde art. 126nd verzoeken), misbruik van bijstandsuitkeringen, RIEC verzoeken, enzovoorts.

Door het op nauwkeurige wijze vastleggen van deze gegevens, kunnen over een bepaalde periode wellicht bepaalde trends in beeld worden gebracht, bestuurlijke informatie worden verstrekt, en mogelijke andere relevante informatie worden verzameld.

Als laatste wordt hier nog genoemd dat deze applicatie dient als een van de bronnen voor de Anti fraude Box (A.

In de handleiding worden de diverse werkstromen beschreven, welke autorisaties benodigd kunnen zijn om met de applicatie te kunnen werken.

Deze applicatie is een voortzetting van dagboek PIT (oud) zoals dat vanaf 2002 door de (voorheen) Belastingdienst/Rijnmond en thans kantoor Rotterdam – Dordrecht is ontwikkeld en gebruikt. De laatste jaren is het 'oude' PIT dagboek in gebruik bij meerdere kantoren en vormde het de rol van landelijk centraal register voor de VTA / systeemfraude.

Autorisaties.

De autorisaties dienen te worden aangevraagd bij Toepassingsbeheer – IM op je kantoor. Hiertoe dient je M2 aan te geven welke rol je als gebruiker voor dagboek FSV dient te krijgen. Je naam, user-id en sap nummer dienen te worden opgenomen in de applicatie.

Autorisatie matrix

Er is sprake van onderstaande autorisaties:

- Balie medewerker (BM)
- Medewerker raadplegen (MR)
- Medewerker raadplegen aangiftefraude (MRA)
- Medewerker raadplegen B.I. (MRB)
- Behandelaar (B)
- Senior behandelaar (SB)
- Platform gebruiker / beheerder (PG/B)
- Special (BCA) (S)
- Behandelaar aangiftefraude (BA)

Zie excellijst waarin de 'rollen' en bijbehorende taken zijn weergegeven.

Baliemedewerker:
Medewerker kan dagboek FSV raadplegen of een subject (signaal) voorkomt. Komt subject niet voor, dan verschijnt deze melding op scherm. Komt subject wel voor, dan verschijnt deze melding op scherm. Baliemedewerker kan nu afhankelijk van signaal, nader stappen ondernemen. Nadere info is niet uit dagboek FSV voor hem/haar te verkrijgen. Dank aan geheimhouding en bijv. aan tonen scherm aan subject.

Medewerker raadplegen:
Medewerker kan alleen het dagboek FSV raadplegen of een subject/signaal voorkomt. Ook kan hij/zij een overzicht hiervan maken en exporteren naar Excel. Voorbeeld van dit soort medewerker: fraudezorgmedewerker, Stella medewerker; e.d.

Medewerker raadplegen aangiftefraude:
Medewerker kan alleen het dagboek FSV raadplegen > werkstroom 'aangiftefraude' < of een subject/signaal voorkomt. Ook kan hij/zij een overzicht hiervan maken en exporteren naar Excel. Voorbeeld van dit soort medewerker: fraudezorgmedewerker, stella medewerker; e.d.

Medewerker raadplegen b.i.:
Medewerker kan alleen het dagboek FSV raadplegen of een subject/signaal voorkomt. Ook kan hij/zij een overzicht hiervan maken en exporteren naar Excel. Deze medewerker gebruikt de informatie hoofdzakelijk ten behoeve van de Bestuurlijke Informatie. Bijvoorbeeld: leidinggevende, projectleiders, e.d.

Behandelaar:
Medewerkers van specials (fraudeteams, team bijzonder aanpak, enzovoorts). Kan alle subjecten/signalen opvoeren, muteren, behandelen.

Senior behandelaar:
Medewerkers van specials (fraudeteams, team bijzonder aanpak, enzovoorts). Kan alle subjecten/signalen opvoeren, muteren, behandelen. Als extra, kan hij/zij regionale projecten benoemen / toevoegen in bestand en hij/zij kan signalen verwijderen.

Beheerder/platform gebruiker:
Deze medewerker kan de diverse lijsten beheren/muteren.

Special (BCA):
Rol bestemd voor medewerkers van BCA. Gericht op toezicht houden op voortgang behandelingen signalen en verkrijgen van b.i.

Behandelaar aangiftefraude:
Medewerkers die zich alleen maar bezighouden met VT-fraude / systeemfraude IH. Zij kunnen signalen opvoeren, muteren en behandelen. Ook het 'lijstwerk' van VTA team Limburg kan door deze medewerkers worden behandeld.

bylage 2

Applicatie	Rol	Omschrijving
FSV	Baliemedewerker	FSV Baliemedewerker
FSV	Behandelaar	FSV Behandelaar
FSV	Behandelaar aangiftefraude	FSV Behandelaar aangiftefraude
FSV	Beheerder	FSV Beheerder
FSV	Raadpleger	FSV Raadpleger
FSV	Raadpleger aangiftefraude	FSV Raadpleger aangiftefraude
FSV	Raadpleger aangiftefraude met B.I.	FSV Raadpleger aangiftefraude met B.I.
FSV	Senior Behandelaar	FSV Senior behandelaar
FSV	Special	FSV Special

Benodigdheden
AAA: aug_FSV_BalieMedewerker
AAA: aug_FSV_Behandelaar
AAA: aug_FSV_BehandelaarAangiftefraude
AAA: aug_FSV_Beheerder (platformgebruiker)
AAA: aug_FSV_Raadpleger
AAA: aug_FSV_RaadplegerAangiftefraude
AAA: aug_FSV_RaadplegerAangiftefraudeMetBI
AAA: aug_FSV_SeniorBehandelaar
AAA: aug_FSV_Special

Wie:
alleen medewerkers klantendienst (inclusief Beltel)
alle medewerkers werkzaam in fraudeteams/specials/teams bijzonder aanpak (inclusief Toeslagen)
alleen medewerkers belast met VTA / systeemfraudeposten (project 1043) inclusief Toeslagen. VTA team (Lim
een medewerker maximaal per kantoor (inclusief Toeslagen)
Stella medewerkers / fraudezorgmedewerkers (klantendienst)
alleen medewerkers belast met VTA / systeemfraudeposten (project 1043) (inclusief Toeslagen)
bestemd voor projectleiders, M2, medewerkers belast met generen bestuurlijke informatie
speciaal aangewezen medewerkers werkzaam in fraudeteams/specials/teams bijzonder aanpak en belast met
bestemd voor medewerkers van BCA. Gericht op toezicht houden op voortgang behandelingen signa

iburg)

VTA / systeemfraudeposten (project 1043) (inclusief Toeslagen)
len en verkrijgen van b.i

bȳlage 3

Autorisaties

De autorisaties dienen te worden aangevraagd bij Toepassingsbeheer – IM op je kantoor. Hiertoe dient je M2 aan te geven welke rol je als gebruiker voor dagboek FSV dient te krijgen. Je naam, user-id en sap nummer dienen te worden opgenomen in de applicatie.

Autorisatie matrix

Er is sprake van onderstaande autorisaties:

- Balie medewerker (BM)
- Medewerker raadplegen (MR)
- Medewerker raadplegen aangiftefraude (MRA)
- Medewerker raadplegen B.I. (MRB)
- Behandelaar (B)
- Senior behandelaar (SB)
- Platform gebruiker / beheerder (PG/B)
- Special (BCA) (S)
- Behandelaar aangiftefraude (BA)

Zie excellijst waarin de 'rollen' en bijbehorende taken zijn weergegeven.

Baliemedewerker: B_DV-02
Medewerker kan dagboek FSV raadplegen of een subject (signaal) voorkomt. Komt subject niet voor, dan verschijnt deze melding op scherm. Komt subject wel voor, dan verschijnt deze melding op scherm. Baliemedewerker kan nu afhankelijk van signaal, nader stappen ondernemen. Nadere info is niet uit dagboek FSV voor hem/haar te verkrijgen. Dank aan geheimhouding en bijv. aan tonen scherm aan subject.

Medewerker raadplegen: B_tz-mkb-50 voor MKB
Medewerker kan alleen het dagboek FSV raadplegen of een subject/signaal voorkomt. Ook kan hij/zij een overzicht hiervan maken en exporteren naar Excel. Voorbeeld van dit soort medewerker: fraudezorgmedewerker, Stella medewerker; e.d.

Met name wordt hier genoemd de medewerker van de **invordering**. Het is belangrijk dat hij/zij informatie over een subject ter beschikking heeft of kan lezen ten behoeve van de invordering (invorderingsmaatregelen).

Medewerker raadplegen aangiftefraude: B_tz-mkb-51 voor MKB
Medewerker kan alleen het dagboek FSV raadplegen > werkstroom 'aangiftefraude' < of een subject/signaal voorkomt. Ook kan hij/zij een overzicht hiervan maken en exporteren naar Excel. Voorbeeld van dit soort medewerker: fraudezorgmedewerker, stella medewerker; e.d.

Medewerker raadplegen b.i.: B_tz-mkb-52 voor MKB
Medewerker kan alleen het dagboek FSV raadplegen of een subject/signaal voorkomt. Ook kan hij/zij een overzicht hiervan maken en exporteren naar Excel. Deze medewerker gebruikt de informatie hoofdzakelijk ten behoeve van de Bestuurlijke Informatie. Bijvoorbeeld: leidinggevende, projectleiders, e.d.

Behandelaar: B_tz-mkb-53 voor MKB
Medewerkers van specials (fraudeteams, team bijzonder aanpak, enzovoorts). Kan alle subjecten/signalen opvoeren, muteren, behandelen.

Senior behandelaar: B_tz-mkb-55 voor MKB
Medewerkers van specials (fraudeteams, team bijzonder aanpak, enzovoorts). Kan alle subjecten/signalen opvoeren, muteren, behandelen. Als extra, kan hij/zij regionale projecten benoemen / toevoegen in bestand en hij/zij kan signalen verwijderen.

Beheerder/platform gebruiker: B_tz-mkb-56 voor MKB
Deze medewerker kan de diverse lijsten beheren/muteren.

Special (BCA):
Rol bestemd voor medewerkers van BCA. Gericht op toezicht houden op voortgang behandelingen signalen en verkrijgen van b.i.

Behandelaar aangiftefraude: B_tz-mkb-54 voor MKB
Medewerkers die zich alleen maar bezighouden met VT-fraude / systeemfraude IH. Zij kunnen signalen opvoeren, muteren en behandelen. Ook het 'lijstwerk' van VTA team Limburg kan door deze medewerkers worden behandeld.

bylage 4

Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport

Basispositie AVG van de BD

Versie: Definitief
Documentnummer: 2018-0000107347

Uitgebracht aan

Persoonsgegevens

Den Haag, 8 juni 2018

Auditdienst Rijk
Ministerie van Financiën

Inhoud

Aanleiding van de opdracht (1/2)

In opdracht van directeur IV&D van de Belastingdienst (BD) hebben wij een onderzoek uitgevoerd naar de basispositie AVG van de BD.

Doelstelling van het onderzoek was:

belangrijke onderwerpen te identificeren in het kader van het voldoen aan de AVG die momenteel niet of niet in voldoende mate in de basispositie BD AVG zitten.

Op basis van bovenstaande doelstelling zijn de volgende onderzoeksvragen gedefinieerd:

OV-1 Welke belangrijke onderwerpen/thema's (AVG attentiepunten) ontbreken ten opzichte van het NOREA Privacy Control Framework en is dat verklaarbaar c.q. gebaseerd op goede gronden?

OV-2 Maken alle BD-objecten onderdeel uit van de basispositie? Zo niet, is dat verklaarbaar c.q. gebaseerd op goede gronden?

OV-3 Welke adviezen zijn te geven inzake de diepgang van de onderwerpen /thema's en of BD-objecten die zijn opgenomen in de basispositie AVG?

Aanleiding van de opdracht (2/2)

De context van het onderzoek was:

De Belastingdienst heeft in de 20e halfjaarsrapportage aan de Kamer gecommuniceerd op 25 mei 2018 niet aan de AVG te kunnen voldoen. Ook is dit besproken in het Audit Committee van het Ministerie van Financiën, d.d. 7 maart 2018. De Belastingdienst heeft een basispositie geformuleerd die richtinggevend is voor de inzet van de BD ten aanzien van de AVG.

De basispositie omvat de onderwerpen/thema's die de Belastingdienst als eerste wil oppakken. Juistheid en volledigheid van de basispositie zijn essentieel, omdat anders tijd/mensen en middelen niet aan de juiste onderwerpen worden besteed.

Algemeen beeld

1. Alle belangrijke onderwerpen/thema's (AVG attentiepunten) zijn in opzet uitgewerkt bij de Belastingdienst (BD). Vanuit de basispositie zijn werkpakketten gedefinieerd, daarnaast liepen er andere BD projecten. Een belangrijk onderwerp dat niet volledig in de basispositie zit, is het schonen van data/archivering. Dit is overigens wel belegd binnen de BD en de einddatum voor realisatie is eind 2018.

2. Alle organisatieonderdelen van de BD zijn betrokken bij het tot stand komen van de basispositie AVG BD. Ook heeft het programma AVG zelf een aantal controles gedaan om tot een volledige registratie van verwerkingen van persoonsgegevens te komen.

3. Ondanks de kanttekeningen bij het onderzoek zijn toch een vijftal adviezen gegeven. Deze zijn op pagina 10 en 11 beschreven.

Kanttekeningen bij onderzoek (1/2)

Belangrijk uitgangspunt voor de Basispositie AVG BD, vastgesteld 10 oktober 2017, is een uitgevoerde risico analyse in de vorm van een uitvoeringstoets (UTNS). Resultaat hiervan is een beschrijving van een minimale te realiseren positie en een beschrijving van uit te voeren acties voor de korte en lange termijn.

De Basispositie AVG BD is vervolgens beschreven in de volgende 9 elementen, waarbij een relatie naar het UTNS niet expliciet is gemaakt:

1. Toepassingsbereik, fundament en aanpak;
2. Transparantie, inzage en correctie, verwerkingsregister;
3. Accountability;
4. Geautomatiseerde besluitvorming en profilering;
5. Vernietigen van gegevens;
6. Privacy by design en by default;
7. Datalekken;
8. Bewustwording en kennis;
9. Organisatie.

Naast bovengenoemde UTNS is ook het 10 stappenplan van de AP en documentatie van het UWV (lid Manifestgroep) input geweest voor de beschrijving van de Basispositie AVG BD. De basispositie is doorvertaald naar uit te voeren werkpakketten. Deze doorvertaling naar werkpakketten hebben we deels kunnen volgen (kanttekening-1).

Kanttekeningen bij onderzoek (2/2)

De uit te voeren werkpakketten zijn kort aangeduid en op programmaniveau AVG niet nader uitgewerkt. De diepgang van de werkpakketten is daardoor lastig te onderzoeken (kanttekening-2).

Daarnaast hebben wij vastgesteld dat de werkpakketten meer werkzaamheden bevatten dan alleen de geplande acties uit de basispositie. Dit is verklaarbaar als gevolg van de door de BD in de uitvoering gesignaleerde issues en generieke risico's. Bovenstaande had wel tot gevolg dat de onderzoekers gedurende het onderzoek op een aantal momenten aanvullende documenten moesten onderzoeken (kanttekening-3).

OV-1, analyse basispositie (1/2)

Uit het onderzoek naar de basispositie aan de hand van de ontvangen documentatie blijkt dat:

- De thema's vanuit het 10 stappenplan AP in beeld zijn bij de BD en uitgewerkt middels de werkpakketten of in andere lopende BD projecten. Programma AVG houdt regie op de eigen werkpakketten;
- Een aantal acties (UTNS) niet expliciet in werkpakketten zijn opgenomen, maar deze zijn grotendeels alsnog wel geadresseerd;
- De actie "Schonen van data/archivering" doorgeschoven is naar duurzaam compliant BD (van korte termijn naar lange termijn). In de beleidsnotitie (d.d. 18 mei 2018) is een einddatum voor realisatie van eind 2018 opgenomen;
- De eventuele acties inzake "Internationale gegevensuitwisseling (art.44 – 50)" niet expliciet zijn vastgelegd. In de beleidsnotitie (d.d. 18 mei 2018) is een einddatum voor realisatie van eind 2018 opgenomen;
- De acties inzake de volgende rechten van betrokkene (gegevenswissing (art. 17), beperking (art. 18), overdraagbaarheid van gegevens (art. 20) en bezwaar (art. 21)) niet expliciet vastgelegd zijn in een werkpakket. In de beleidsnotitie is hiervoor een motivatie opgenomen.

OV-1, analyse basispositie (2/2)

- De gegevensverwerkingen door BD voor derden, bijvoorbeeld gebruik printstraat, niet duidelijk is benoemd in de basispositie en hoe de BD hier mee omgaat;
- De grondslag toestemming van de betrokkene is niet verder uitgewerkt (art. 7). Dit bleek voor de BD niet van belang (voortschrijdend inzicht). Dit was niet expliciet vastgelegd in een werkpakket, maar is inmiddels wel opgenomen in de beleidsnotitie (d.d. 18 mei 2018) als beleidslijn (gg);
- Over de omgang met het verwerken van bijzondere categorieën van persoonsgegevens (art. 9) geen specifieke uitwerking in een werkpakket is opgenomen, maar ook dit is inmiddels opgenomen in de beleidsnotitie.

<u>Algeheel beeld uit onderzoek:</u>

Alle belangrijke onderwerpen/thema's (AVG attentiepunten) zijn in opzet uitgewerkt bij de Belastingdienst (BD). In de basispositie, uitgewerkt in werkpakketten, zijn niet alle onderwerpen opgenomen. Dit is verklaarbaar, omdat deze zijn opgenomen in andere BD projecten, niet relevant zijn voor de BD of omdat de realisatie gepland is na 25 mei. Deze verklaring is vastgelegd in de beleidsnotitie van 18 mei 2018.

OV-2, analyse BD objecten

Onderzoeksvraag 2 was gericht op twee subvragen:

1. Hoe weet het programma AVG dat alle BD onderdelen aangehaakt zijn?
2. Hoe weet het programma AVG dat alle bedrijfsprocessen in beeld zijn?

Ad 1.) Alle organisatieonderdelen van de BD zijn betrokken bij het tot stand komen van de basispositie AVG BD. Aan de voorkant, bij de risico-analyse, die via de standaard UTNS procedure is verlopen, waarbij alle BD onderdelen medio 2017 waren aangehaakt en aan de achterkant omdat de basispositie besproken is in de MT's van de BD.

Ad 2.) De bedrijfsprocessen worden geïnventariseerd in de basispositie AVG BD (werkpakket 1.3.2.2). De borging van de volledigheid van de inventarisatie wordt bereikt middels het gebruik van de landschapskaart (gebaseerd op de enterprise architectuur van de nieuwe domeinen) en door een aansluiting te maken met de administratie van WBP meldingen. Wij hebben de resultaten van bovenstaande checks niet geverifieerd.

NB, de juistheid van de verwerkingsregistratie wordt in opzet afgedekt door de beoordeling door de FG (werkpakket 1.3.2.2.1). Tevens heeft de BD een verbeterplan aangekondigd. Dat verbeterplan is erop gericht tot een publicabel register te komen en richt zich op semantiek en inhoudelijke juistheid van de registratie.

OV-3, analyse diepgang (1/2)

Bij ons onderzoek zijn wij uitgegaan van het niveau van de uitwerking zoals vermeld in de basispositie en de daaruit voortkomende werkpakketten. Dit heeft geleidt tot de volgende adviezen:

1. Profilering is nieuw binnen de AVG en geautomatiseerde individuele besluitvorming waaronder profilering speelt een rol binnen het primaire proces van de BD. Bijvoorbeeld bij de bepaling of een belastingaangifte Inkomstenbelasting geautomatiseerd wordt verwerkt of nog aanvullend handmatig wordt gecontroleerd. De BD heeft hierover een beleidslijn geformuleerd. Omdat dit een open norm is en het nog onbekend is hoe de rechter en de AP hierover denken adviseren wij de BD om hier blijvende aandacht aan te besteden;

2. Het auditproces is aangeduid in werkpakket 1.3.6.1. Wij adviseren om dit op te nemen in concrete auditplannen en hier voldoende auditcapaciteit voor in te ruimen;

3. Pseudonimisering is benoemd in het UTNS, maar niet uitgewerkt in werkpakketten. Wij adviseren beleid inzake Pseudonimisering te ontwikkelen en dit te integreren met bestaand Informatiebeveiligingsbeleid (Handboek Beveiliging Belastingdienst, HBB);

OV-3, analyse diepgang (2/2)

4. Privacy by design/default (werkpakket 1.3.8) ook meenemen bij aanbestedingen. Nu nog niet expliciet benoemd. In het recentelijk vastgestelde privacybeleid Financiën is wel een opmerking over inkoop gemaakt. Wij adviseren na te gaan of dit voldoende is uitgewerkt in de bestaande inkoopprocedures;

5. PDCA cyclus voor privacy incl. documenten, bijv. privacy statement niet expliciet beschreven (werkpakket 1.3.4.1.1 en 1.3.4.1.3). Het inrichten van een PDCA cyclus is als uitgangspunt benoemd in het privacybeleid van het Ministerie van Financiën. Wij adviseren na te gaan of dit voldoende uitgewerkt is in bestaande procedures en concreet belegd is in de organisatie.

Vervolg programma AVG

Op 25 mei 2018 is de BD nog niet volledig AVG compliant. Wij adviseren veel aandacht te geven aan het decharge document van het programma om te laten zien dat de BD inzicht heeft in de nog openstaande punten en daarop concrete acties heeft belegd.

Concreet betekent dit:

- Afwikkeling van alle UTNS acties m.n. die niet zichtbaar opgenomen zijn in de werkpakketten, zoals: Inrichten voorziening voor (digitale) identificatie/authenticatie van betrokkenen die een verzoek indienen, Inzage/correctierecht (aanpassen van de websites en de portals, informeren derde partijen bij correcties, *nu lange termijn actie*);
- Duidelijke realistische tijdlijnen en verantwoordelijken benoemen van de te nemen initiële acties voor de implementatie van de AVG en het inrichten en beleggen van het reguliere beheer;
- De stand van zaken inzake de AVG implementatie valideren en vastleggen welke keuzes gemaakt zijn;
- Vastleggen van de 'lessons learned' en overdracht van de regie aan de procesverantwoordelijke AVG;
- Mogelijkheden onderzoeken voor aansluiting bij goedgekeurde gedragscodes en certificeringsmechanismen (overweging 98-100 bij AVG).

Verantwoording onderzoek

Werkzaamheden

De volgende aanpak is gehanteerd:

- Gesprekken voeren met leden kernteam AVG;
- Bestuderen van diverse documenten;
- Beoordelen totstandkoming UTNS;
- Beoordelen UTNS ten opzichte van basispositie en werkpakketten;
- Aansluiten werkpakketten met NOREA Privacy Control Framework;
- Analyseren uitkomsten in relatie tot onderzoeksvragen.

Bovenstaande aanpak betekent dat we alleen naar de opzet van de basispositie hebben gekeken, zoals beschreven door het programma AVG.

Verantwoording onderzoek

Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Deze audit betreft een onderzoeksopdracht. Derhalve wordt in dit rapport geen zekerheid verschaft, omdat het een onderzoeksopdracht betreft.

Verspreiding rapport

De opdrachtgever, Persoonsgegevens, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

Verantwoording onderzoek

Dit onderzoeksrapport is opgesteld door:

Persoonsgegevens

Den Haag, 8 juni 2018

Auditdienst Rijk

Management reactie (1/3)

Op 8 juni hebben we de concept ontvangen van het onderzoeksrapport naar de basispositie AVG bij de BD. De opdracht voor dit onderzoek is voort gekomen uit de wens van het management van de BD om meer inzicht te hebben in de mate van de compleetheid van de basispositie t.o.v. de AVG. Met het algeheel beeld, zoals verwoord in de rapportage, wordt voldaan aan deze behoefte.

Algeheel beeld zoals verwoord in de conceptrapportage:

- *Alle belangrijke onderwerpen/thema's (AVG attentiepunten) zijn in opzet uitgewerkt bij de Belastingdienst (BD). In de basispositie, uitgewerkt in werkpakketten, zijn niet alle onderwerpen opgenomen. Dit is verklaarbaar, omdat deze zijn opgenomen in andere BD projecten, niet relevant zijn voor de BD of omdat de realisatie gepland is na 25 mei. Deze verklaring is vastgelegd in de beleidsnotitie van 18 mei 2018.*

In de bespreking van de stand van zaken implementatie AVG in het directieteam BD d.d. 24-5-2018 is vastgesteld dat voor zover de BD nog niet volledig voldoet aan de AVG, activiteiten zijn geadresseerd gericht op compliance op of voor 25 mei 2019. De acties verwijzen naar een gedetailleerde opsomming van activiteiten, toegewezen aan actiehouders, gericht op een goede overdracht van project naar de lijn, de invulling van de open normen en gericht op het volledig voldoen aan de door de AVG gestelde eisen. Op deze manier bestaat inzicht in en is besturing mogelijk van het verder verbeteren van de compliance met de AVG.

Management reactie (2/3)

Het algeheel beeld van het onderzoek bevestigt dat in opzet alle relevante aspecten van de AVG zijn uitgewerkt. De basispositie is een belangrijk instrument geweest voor de projectmatige besturing van de implementatie ondersteuning. De door het DT vastgestelde acties zijn gericht op het opheffen van de deficiëntie met de AVG zelf. De basispositie is voor dit vervolg niet meer relevant.

De aanbevelingen in de rapportage, met inbegrip van de opmerkingen hieronder, nemen we over en worden verwerkt in de voor 25 mei 2019 uit te voeren acties.

De aanbevelingen in detail:

Ad Auditproces

Deze aanbeveling nemen we over en wordt opgenomen in het verbeterplan rondom het verwerkingenregister, waarnaar al in de paragraaf "Analyse BD objecten" wordt verwezen.

Ad Pseudonimisering

Deze aanbeveling nemen we over en is geadresseerd in het overzicht van activiteiten uit te voeren voor 25-5-2019.

Management reactie (3/3)

Ad Privacy by design/default bij aanbestedingen

Advies wordt overgenomen.

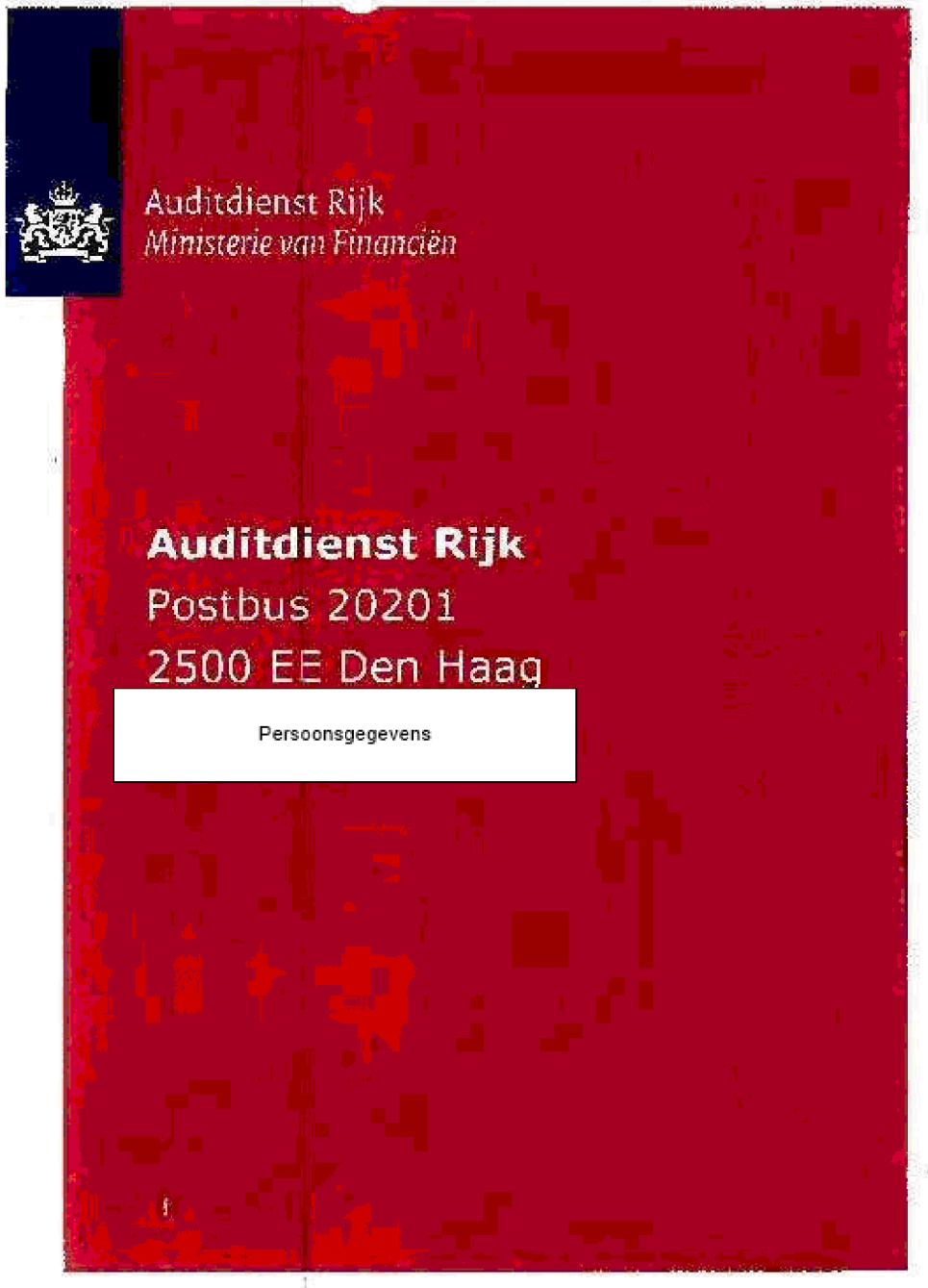
Ad PDCA cyclus voor privacy in afstemming met MinFin

Advies wordt overgenomen en krijgt een plek in het domeinoverleg privacy dat binnen MinFin met vertegenwoordigers van alle onderdelen wordt georganiseerd.

Ad Profilering

Het onderwerp geautomatiseerde besluitvorming met inbegrip van profilering is veelbesproken en is een sprekend voorbeeld van een open norm in de AVG. In de reeds vermelde beleidsnotitie heeft de BD de open normen geconcretiseerd. Ook voor geautomatiseerde besluitvorming is dat, in afstemming met BJZ, DGFZ en de FG, gebeurd.

Ter uitvoering van het kabinetsstandpunt bij het WRR-rapport over Big data worden in werkgroepen rijksbrede richtsnoeren voor transparantie over big data analyses en voor inzicht in algoritmen uitgewerkt. De Belastingdienst neemt hierin deel en zal mede op basis van deze rijksbrede richtsnoeren de beschreven praktijk waar nodig aanpassen of aanvullen. Er is daarmee blijvende aandacht voor deze problematiek.


Auditdienst Rijk
Ministerie van Financiën
Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
Persoonsgegevens

bÿlage 5

Digitaal aangeleverd

bylage 6

Digitaal aangeleverd

bylage 7

Digitaal aangeleverd

bylage 8

Digitaal aangeleverd

bylage 9

Digitaal aangeleverd

bylage 10

Digitaal aangeleverd

bylage 11

Digitaal aangeleverd

bylage 12

Digitaal aangeleverd

bylage 13

Digitaal aangeleverd

bÿlage 14

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Persoonsgegevens Ik ben last-minute ingevlogen omdat Persoonsgegevens onverwachts niet blijkt te kunnen. Persoonsgegevens is de man die in het verleden ook het een en ander heeft meegekregen. Ikzelf ben sinds mei betrokken bij het project als Persoonsgegevens vanuit MKB voor het hele FSV verhaal. Ik heb wel het nodige mee gekregen, maar niet uit eigen ervaring. Behalve dan sinds mei.

Persoonsgegevens

Ik ben Persoonsgegevens ik werk binnen de Shared Service Organisatie Financieel en Managementinformatie als Persoonsgegevens identity and accessmanagement. Ik ben sinds 2013 werkzaam binnen deze afdeling en in de vorige organisatiestructuur werkzaam geweest in dit vakgebied.

Persoonsgegevens

Jullie hebben ook nog documenten opgestuurd. Vlak voor deze vergadering. Die heeft Persoonsgegevens gedownload en ook naar de andere deelnemers doorgestuurd van ons. Het waren wel veel stukken. Dus wij hebben ze niet allemaal doorgenomen. Overigens zijn het wel herkenbare stukken. Wel die wij wel eens eerder voorbij hebben zien komen. Maar ik ben ook wel benieuwd in wat voor context jullie die hebben gedeeld vooraf.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik heb dus geen van die stukken. Voor mij zijn die vragen ook volkomen een raadsel, maar dat hoor ik dan wel wanneer het zover is.

Persoonsgegevens

Ik zet ze nog even naar je door ondertussen, maar ik denk niet dat je er iets aan mist.

Persoonsgegevens

Misschien toelichtend vooraf. Ik heb met Persoonsgegevens vooraf doorgesproken van zouden wij niet nog een extra gesprek kunnen voeren met de Autoriteit Persoonsgegevens omdat wij merkten dat wij het moeilijk vonden om de vragen rondom de autorisaties goed te beantwoorden. Ik hoop dat we dat dus nu wel beter kunnen doen. Ook

Overzicht van opmerkingen bij Microsoft Word - Verklaringen telefonisch afgelegd door Belastingdienst op 2 december 2020

Pagina: 3

T Nummer: 1	Auteur	Persoonsgegevens	Onderwerp: Ingevoegde tekstDatum: 21-12-2020 17:11:31 +01'00'

ook