Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Niets anders als een gewone gebruiker. Vanuit logging perspectief is het is gewoon een gebruiker die een scherm aanroept. Die kun je ook terugzien in de logging van de 30 juni want Persoonsgegevens Persoonsgegevens is functioneel beheerder en de activiteit die Persoonsgegevens die dat heeft gedaan, dat wordt gelogd als functioneel beheerder. Dat zijn dezelfde dingen als van andere gebruikers. Andere schermen dat wel, maar de layout is hetzelfde.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat past niet in de procedure zoals die afgesproken is met het datacenter. Wij nemen even aan dat het om de technisch beheerder van het data center gaat, want andere technisch beheerders kunnen niet bij de data. De applicatiebeheerder zit aan de development kant, hebben geen toegang tot productiegegevens. Het moet gaan om de technische beheerders bij de exploitatie afdeling van DCS, datacenter services. Die zijn gebonden aan strikte procedures en hun handelingen worden gelogd. Dus ja, ze kunnen bij de data. Ja, ze kunnen de database volledig om zeep helpen. Dat valt onder hun verantwoordelijkheid, maar dat wordt wel gelogd. En dan heb je direct of een back-up terug te zetten, zodat wij kunnen zien wat er gebeurd is, of de gebruiker gaat klagen van 'ik ben mijn gegevens kwijt'. Dan kunnen zij een back-up terug zetten. Dat is een reden waarom je back-ups maakt. Ook al zou je dat kunnen, met welke doel moet je even afvragen en wat bereik je ermee. Technisch kan het. Dat hoort bij de functie van een DBA. Ik ben niet blij met de zinsnede in de GEB want het is niet gebaseerd op de werkelijkheid, het is een theoretisch exercitie geweest.

Persoonsgegevens

En de DBA heeft in deze ook absoluut geen kennis van de inhoud van de database. Wat er in staat en hoe hij dat moet interpreteren, daar heeft hij absoluut geen kennis van.

Persoonsgegevens

Nee. Die opmerking in de GEB die herken ik niet praktijk.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, absoluut. Hij moet het doen of in opdracht van bijvoorbeeld applicatie beheer, van er zit iets fout in de database, er is een mutatiefout, veldje A moet vervangen door veldje B. Dan maakt de ontwikkelafdeling een update script als het goed is van vervang in de database op dat en dat veld record A door record B en die handeling wordt dan door zo'n DBA uitgevoerd.

Persoonsgegevens

Die opdracht komt altijd vanuit functioneel beheer.

Persoonsgegevens

Exact.

Persoonsgegevens

Zij kennen niet de techniek erachter, ze komen bij ons met het verzoek. Wij bouwen daarvoor dan een script en verzinnen een manier om dat te testen. Leveren we dat script op aan functioneel beheer en functioneel beheer maakt de afspraken om het script te draaien met de DBA. Op die manier is het hele proces dan ook weer gelogd.

Persoonsgegevens

Op basis van incidentmeldingen, want dat doe je niet even voor de gein. Dat loopt netjes via het log proces van de helpdesk.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Nee. Op het moment hij toegang wil tot die database, dan moet hij dat op basis van een incidentnummer doen. Dan zou je nog een incidentennummer kunnen faken, van ik bedenk een nummer want ik heb net storing 1001 gehad, dus ik zet nu dat wij storing 1002 moeten oplossen. Dan krijg je toegang tot die database op basis van storing 1002. Op dat moment loopt er een logging mee met alle handelingen die de beheerder doet. Als hij dan kwaadwillend alles weg gooit, dan is de database leeg, maar dan hebben wij onze back-ups om dat te herstellen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Nee, dat is een dedicated tooling waarin wordt vastgelegd dat beheerder X geautoriseerd wordt om toegang te krijgen tot het platform waar die server op staat. En dat hij dus ook het DBA wachtwoord krijgt van die sequel server, want hij kent die wachtwoorden niet. Dat is een van de basis beveiligingen. Beheerders kennen niet standaard het wachtwoord van die machine. Die krijgt hij geautomatiseerd toegekend, zogenaamde PAM tooling, Privileged Access Management. Er zit een hele kluisprocedure aan vast. Als je hogere beheerrechten hebt dan normaal, zit er een procedure aan vast om te zorgen dat jij niet dus standaard beschikt over die wachtwoorden. Dat kan ook niet, want we hebben duizenden sequel servers. Je kan niet verwachten dat een beheerder van al die duizenden sequel servers de wachtwoorden kent. Dat is onmogelijk. Dat is afgeschermd met een extra laag tooling. Daar vindt ook auditing op plaats door de ADR, juist vanwege het hoog risico karakter ervan.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Daar kan ook niemand bij, alleen bij integriteitsonderzoek. Je gaat niet je medewerkers volgen omdat je hem wilt volgen. Dan moet je hem ergens van verdenken. Pas als er een integriteitsonderzoek wordt gestart, kunnen we bij die logging. Nou niet wij maar de mensen die bij dat onderzoek betrokken zijn.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

De generieke tooling heet PAM tooling, Priviliged Acces management. Maar welke tool we daar als Belastingdienst voor gebruiken weet ik niet. Waarschijnlijk is die ook platform afhankelijk, want ik kan mij niet voorstellen dat er één tool bestaat die voor alle platforms die de Belastingdienst heeft.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Een deel van die logging zoals de heer Persoonsgegevens schetst, dat herken ik wel maar dat is specifiek voor Windows sequel server ook zo geregeld dat die specifiek voor die database een wachtwoord krijgt. Volgens mij zit het in zijn profiel of rol dat hij bij de database mag, maar de toegang tot die database wordt absoluut gelogd en wat hij daarin doet ook.

Persoonsgegevens

Het kan zijn dat voor de sequel server die hier gebruikt wordt net een iets andere procedure geldt, maar het wordt standaard gelogd. Het zou niet best zijn als wij on-gelogd beheerders toegang tot systemen geven. Dat is voor de financiële stroom van belastingdienst niet verantwoordt. Als wij het niet kunnen garanderen hoe het geld tot stand gekomen is en de opbrengsten tot stand gekomen zijn, dan hebben wij een uitdaging.

Persoonsgegevens

Ik kom het in de praktijk in deze ook tegen van als je zegt 'kun je dat even voor mij uitvoeren', dat je dat alleen doet op basis van een opdracht. Je maakt een incident of een werkorder, dan wordt het gelogd en dan zit het in zijn proces. Dan heeft hij toestemming om bij die database te mogen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Die vraag kun je dan gewoon aan ons stellen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Die heb ik vertaald als hoe werkt de logging in Microsoft sequel server. Ik ga even uitzoeken hoe dat werkt.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, kan je dat in de logging terugvinden.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Hoe die naamgeving veranderd is, of die überhaupt veranderd is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Die heb ik ook staan.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik heb nog even een vraag. Wanneer willen jullie deze antwoorden? En er waren twee documenten die jullie voor dit overleg nog wenste, die heb ik tijdens het overleg gestuurd. Willen jullie die nog apart geüpload hebben naar de bestandenpostbus of is dit op dit moment voldoende?

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

De antwoorden mogen ook via de mail denk ik.

Persoonsgegevens

Wat makkelijk is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: dinsdag 15 september 2020 09:59
Aan: Persoonsgegevens
Onderwerp: RE: Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

Hierbij bevestig ik dat ik het bestand 'Verklaringen telefonisch .... 20 augustus 2020' in goede orde heb ontvangen via de bestandenpostbus. Het toegestuurde wachtwoord was correct.

Ik zal u uiterlijk 28 september 2020 informeren over eventuele feitelijke onjuistheden in de verklaringen.

Met vriendelijke groet,

Persoonsgegevens

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

Persoonsgegevens

Van: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Verzonden: maandag 14 september 2020 19:38
Aan: Persoonsgegevens @minfin.nl>
Onderwerp: Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

Op 20 augustus jl. heeft de Autoriteit Persoonsgegevens in het kader van het onderzoek naar de FSV applicatie van een aantal medewerkers van de Belastingdienst telefonisch verklaringen afgenomen aangaan de logging. De uitwerking van deze verklaringen heb ik zojuist in de Bestandenpostbus geupload. Het betreft het document *Verklaringen telefonisch afgelegd door Belastingdienst op 20 augustus 2020v.pdf*. Kunt u de ontvangst van dit document aan mij bevestigen?

Ik verzoek u vriendelijk om uiterlijk 28 september 2020 aan te geven of er feitelijke onjuistheden in de verklaringen staan. Omdat de verklaringen woordelijk zijn uitgewerkt is er sprake van spreektaal, met soms wat kromme zinnen. Dit is niet erg als ze maar feitelijk juist zijn. De opmerkingen van de Belastingdienst zullen niet leiden tot wijziging van de verklaringen, maar worden wel als bijlage toegevoegd aan het document.

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: vrijdag 18 september 2020 09:17
Aan: Persoonsgegevens
Onderwerp: RE: Aanlevering uitgewerkte verklaringen 30 juni 2020 via Bestandenpostbus

Geachte mevrouw Persoonsgegevens

Allereerst bevestig ik hierbij de ontvangst van de volgende vier pdf-documenten met de reactie van de verschillende medewerkers van de Belastingdienst:

Verklaringen afgelegd door Belastingdienst onderzoek ter plaatse op 30 juni 2020 -
Verklaringen afgelegd door Belastingdienst onderzoek ter plaatse op 30 juni 2020 -
Verklaringen afgelegd door Belastingdienst onderzoek ter plaatse op 30 juni 2020 -
Verklaringen afgelegd door Belastingdienst onderzoek ter plaatse op 30 juni 2020 -
Persoonsgegevens

constateer dat er naast de gevraagde feitelijke onjuistheden er door Persoonsgegevens Persoonsgegevens ook algemene opmerkingen zijn gemaakt over het onderzoek ter plaatse op 30 juni 2020 en het verslag met verklaringen. Hierop wil ik als volgt reageren:

- De opmerking dat niet is vastgelegd in het verslag dat de uitwerking woordelijk is gedaan en niet zakelijk zoals eerder aangekondigd: *dit is aangegeven in mijn mail aan u van 25 augustus 2020 waarmee de AP de verklaringen afgelegd op 30 juni heeft aangeleverd. De e-mail wordt opgenomen in het dossier.*
- De constatering dat in het verslag niet is opgenomen dat de cautie niet gesteld is en het recht op bijstand wel is gegeven: *dit is opgenomen in de Verklaring van Ambtshandelingen van de OTP van 30 juni die door de AP is opgesteld. Deze VvA wordt opgenomen in het dossier.*
- De opmerking dat ik beloofd zou hebben dat de uitwerking van de verklaringen binnen 10 werkdagen zouden worden opgeleverd: *ik ontken deze termijn genoemd te hebben*
- De opmerking dat het een verhoor bleek en geen (informeel) beantwoorden van vragen over de werking van FSV: *ik laat het aan u als contactpersoon voor AP onderzoeken (met daarmee ook de nodige ervaring) om hierover de benodigde uitleg te geven aan de betrokken medewerkers.*

Ik vertrouw erop u hiermee te hebben geïnformeerd.

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

'Privacy gaat iedereen wat aan'

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: vrijdag 18 september 2020 09:24
Aan: Persoonsgegevens
Onderwerp: RE: Opvragen FSV logbestanden

Geachte mevrouw Persoonsgegevens

Hierbij bevestig ik de eerdere ontvangst van het bestand *FSV_20190305.zip* met daarin 317 dagelijkse logbestanden: FSV_20190304.txt t/m FSV_20200227.txt

Vriendelijke groeten,
Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: maandag 14 september 2020 17:12
An: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
CC: Persoonsgegevens @autoriteitpersoonsgegevens.nl>; Persoonsgegevens
Persoonsgegevens @minfin.nl>
Onderwerp: RE: Opvragen FSV logbestanden

Geachte mevrouw Persoonsgegevens

In vervolg op onderstaand bericht informeer ik u dat ik de gevraagde logbestanden aangeboden heb via de bestandenpostbus in een zipbestand.

Ik vertrouw erop u hiermee van dienst te zijn.

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

Van: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Verzonden: vrijdag 4 september 2020 13:25
Aan: Persoonsgegevens @minfin.nl>; Persoonsgegevens
Persoonsgegevens @minfin.nl>
CC: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Onderwerp: Opvragen FSV logbestanden

Geachte mevrouw Persoonsgegevens

Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: maandag 28 september 2020 21:10
Aan: Persoonsgegevens
Onderwerp: onderzoek FSV - reactie op Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

In vervolg op uw bericht van 14 september 2020 informeer ik als volgt.

De heer Persoonsgegevens heeft geen opmerkingen of aanvullingen.

De heer Persoonsgegevens heeft enkele opmerkingen gemaakt.
Het bestand met opmerkingen heb ik aangeboden via de bestandenpostbus.
[het verliep anders dan eerder, ik kon helaas niet zien of het gelukt is.]

Opmerking van de heer Persoonsgegevens
-equel-server moet zijn : SQL-server;
/m-tooling moet zijn : SIEM tooling

Ik vertrouw erop u hiermee van dienst te zijn.

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

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: dinsdag 29 september 2020 09:02
Aan: Persoonsgegevens
Onderwerp: RE: onderzoek FSV - reactie op Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

Dank u voor uw email met daarin de opmerkingen van Persoonsgegevens Ik zie dat het uploaden van de opmerkingen van Persoonsgegevens in de Bestandenpostbus niet is gelukt, zou u het nog een keer kunnen proberen?

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

'Privacy gaat iedereen wat aan'
De privacywet (AVG) zorgt voor meer grip op persoonsgegevens. Weten wat de privacywet voor jou betekent? Kijk op www.hulpbijprivacy.nl.

Van: Persoonsgegevens @minfin.nl>
Verzonden: maandag 28 september 2020 21:10
Aan: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Onderwerp: onderzoek FSV - reactie op Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

In vervolg op uw bericht van 14 september 2020 informeer ik als volgt.

De heer Persoonsgegevens heeft geen opmerkingen of aanvullingen.

De heer Persoonsgegevens heeft enkele opmerkingen gemaakt.
Het bestand met opmerkingen heb ik aangeboden via de bestandenpostbus.
[het verliep anders dan eerder, ik kon helaas niet zien of het gelukt is.]

Opmerking van de heer Persoonsgegevens
-sequel-server moet zijn : SQL-server;
-sym-tooling moet zijn : SIEM tooling

Ik vertrouw erop u hiermee van dienst te zijn.

Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: dinsdag 29 september 2020 10:01
Aan: Persoonsgegevens
Onderwerp: RE: onderzoek FSV - reactie op Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

In reactie op uw bericht heb ik het bestand met de opmerkingen van de heer Persoonsgegevens nog een keer aangeboden via de bestandenpostbus. Het lijkt nu wel gelukt.

Met vriendelijke groet,

Persoonsgegevens

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

Persoonsgegevens

Van: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Verzonden: dinsdag 29 september 2020 09:02
Aan: Persoonsgegevens @minfin.nl>
Onderwerp: RE: onderzoek FSV - reactie op Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

nk u voor uw email met daarin de opmerkingen van Persoonsgegevens Ik zie dat het uploaden van de opmerkingen van Persoonsgegevens in de Bestandenpostbus niet is gelukt, zou u het nog een keer kunnen proberen?

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

AUTORITEIT
PERSOONSGEGEVENS

Verklaringen telefonisch afgelegd door Belastingdienst op 20 augustus 2020

Namens de Autoriteit Persoonsgegevens

Persoonsgegevens

Namens de Belastingdienst

Persoonsgegevens

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Precies, ik denk dat dat het is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Persoonsgegevens mijn functie is officieel externe informatievoorziening hier bij de afdeling GBS. Wij onderhouden applicaties waaronder FSV en nog andere, maar dan met de richtlijnen van DCS.

Persoonsgegevens

Persoonsgegevens Ik ben Persoonsgegevens Ik ben manager Persoonsgegevens Wij zitten inderdaad bij Generieke Businessvoorzieningen Services (GBS). Wij vallen onder het MCC, dat is het Mobile Competence Center. Daar onderhouden wij alle apps van de Belastingdienst en andere overheden. Daar hebben wij allerlei dot.net applicaties Ik ben verantwoordelijk voor al die dot.net applicaties. Dat doen wij voor tien domeinen, tien ketens, waaronder ook de Keten Toezicht waar FSV onder valt.

Persoonsgegevens

Inspectie, controle en toezicht

Overzicht van opmerkingen bij Microsoft Word - Verklaringen telefonisch afgelegd door Belastingdienst op 20 augustus 2020_final

Pagina: 1

Nummer: 1 Auteur: Persoonsgegevens Onderwerp: Markering Datum: 18-9-2020 11:14:40
mijn functie is officieel Expert Informatievoorziening...

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Voor FSV geldt eigenlijk dat het een vrij simpele infrastructuur is, er is een webserver waar de applicatie op wordt gehost. Er is een dedicated webserver voor FSV. Die staat daarop dus alleen, er staan geen andere applicaties op. Er is een aparte SQL-server waar de database van FSV op staat en op die SQL server zitten wel databases van andere applicaties. De toegang van de database is zodanig geregeld dat alleen de applicatie recht heeft op de database, en de DBA van SQL-server.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Sinds kort is er een loadbalancer voor FSV, tenminste de laatste voordat die uitging. Alleen die ene server is de enige host voor die loadbalancer. Er is maar één webserver voor FSV. Toegang tot die applicatie is dan geregeld via het AD, [interferentie en IMS] daar hebben we het een andere keer over gehad. Dat is eigenlijk de globale ingang. Het is niet heel spannend.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, als datareader en datawriter.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik verwacht zo tussen november 2019 en februari 2020. Dat zou ik na moeten kijken wanneer dat expliciet gedaan is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

De reden dat we die loadbalancer er tussen gezet hebben, is dat er certificaten gingen vervallen. Er was een certificaat geïnstalleerd op die webserver zelf om https-verkeer mogelijk te maken. Omdat te vereenvoudigen hebben wij een loadbalancer er tussen gezet waardoor we van een generieke certificaat gebruik konden maken waardoor het onderhoud en beheer eenvoudiger werd. De klant heeft daar geen notie van.

Persoonsgegevens

Dank je wel.

Nummer: 1 Auteur: Persponsgegevens Onderwerp: Opmerking over tekst Datum: 18-9-2020 11:18:18

dat wordt ingericht m.b.v. IMS

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Het http-request staat erin en de status. Een status 200 als het succesvol is en 500 of 400 wanneer er een error optreedt.

Persoonsgegevens

Ik heb het bestand ondertussen voor mij staan. Ik kan het eventueel delen. De twee gevraagde bestanden die de AP graag wilde hebben van de 24ste juli en 30 juni.

Persoonsgegevens

Ja, graag.

Persoonsgegevens

Dan stuur ik ze nu even naar iedereen en dan kunnen we wellicht in de sessie nog even er in kijken.

Persoonsgegevens

Ik vermoed dat in die bestanden nog een usernaam staat wie die request uitvoert, user-id. Geen naam, maar een user-id.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Niet ten aanzien van de applicatie. Niet ten aanzien van de webserver waar het op draait zodanig. De enige plek waar nog logging zou kunnen plaatsvinden, maar dat is compleet buiten mijn scope, dat is op de [1]equel server die een transactie log doet van de transacties die op de databases plaats vinden.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja, dat gaat over die dingen.

Persoonsgegevens

Inspectie, controle en toezicht

Nummer: 1 Auteur: Persoonsgegevens Onderwerp: Opmerking over tekst Datum: 18-9-2020 11:23:24

hier wordt MS SQL Server bedoeld, maar we spreken het uit als 'sequal server'

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Persoonsgegevens ik heb je bestanden ook even toegestuurd. Dan weet je in ieder geval waar het over gaat. Ik heb ze van DCS gekregen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Wat die hier gewoon aangeeft is welke pagina je oproept. Zo zie ik het hoor. Als ik het fout heb, dan hoor ik dat natuurlijk graag. En hier zegt hij dan of het goed is gegaan dat de pagina opgeroepen is. Om 4:33:33 uur zien we 'page not found'-pagina die naar voren komt. Dan zie je daarachter ook een 500 error staan. Hier zie je dus alleen welke pagina die webserver heeft moeten serveren. Die ander log zie je dus vanuit de applicatie zelf welke functie die eigenlijk aangeroepen heeft. Wat over het algemeen dus samen hangt met de webpagina, lijkt het.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Nee.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ik ben even kwijt over welke bestanden we het nu hebben.

Persoonsgegevens

Ik pak ze er even bij, ik stuur ze even door.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat mag voor dit onderzoek, maar dat is wel op een datum waarop de applicatie niet meer in gebruik is. Er zit heel veel ruis in van de applicatie zelf. Daar staat minder informatie in over wat er de users hebben gedaan.

Nummer: 1 Auteur: Persoonsgegevens Onderwerp: Opmerking over tekst Datum: 18-9-2020 11:27:45

Ik kan me niet voorstellen dat de Persoonsgegevens dit heeft gezegd.

Persoonsgegevens

De heer Persoonsgegevens wat u niet weet is dat op 30 juni hebben wij onderzoek van de AP gehad in Den Haag. Daar hebben we gebruikers van de Belastingdienst uitgenodigd om te demonstreren wat er in FSV zat. Er zitten vijf gebruikers in als het goed is en er is heel bewust gekozen dat die dag de server wel in de lucht was, maar dat wist jij weer niet.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is de applicatie logging zoals wij dat in FSV hebben en ook de meeste andere applicaties die wij in onderhoud en beheer hebben met als doel voor incidenten en problems. Deze staat ook zodanig aan dat alle andere activiteiten zoals tracing ook gelogt worden. In dat geval krijg je dus zoals regel één, dat je kunt zien van welke gebruiker op welk moment welke use case raadpleegt. Dus als eerste datum en tijd, dat is het moment waarop die in Nederlandse tijd hem uitvoert. Dan krijg je een streepje met een naam aanduiding voor de gebruikers ID. Gebruikers ID waarmee die inlogt, die staat dan tussen haakjes. Daarmee is die ook bekend binnen het 1B Dat is de gebruikers ID die rechten moet hebben. Dan heeft de applicatie twee momenten dat die logt. Dat is bij het starten van de use case en er is nog een ander moment. Zo'n use case begint ergens en die eindigt ergens. Dan heb je dus een begin startmoment en een beëindigingsmoment. Dan zijn twee momenten binnen hetzelfde request die de applicatie dan logt. Daarom zie je 'trace Start' en 'trace Bind' op regel drie. Dan heb je een use case naam die die opent. Dan is een stukje functionaliteit van de applicatie die mogelijkheden biedt om andere acties uit te voeren. En er wordt gelogd hoe lang die erover duurt, in miliseconden, omdat request voor dat deel af te handelen. Die hebben wij erin staan om de tijden te kunnen monitoren van de applicatie. Soms krijgen we performance klachten, dan wordt er gezegd 'het duurt lang'. Dan willen wij weten, hoeveel users zijn er gelijktijdig binnen een uur of binnen een sectie, binnen een tijdsbestek bezig en wat doet dat met de doorlooptijden van die requests als zodanig. Dat is wat we loggen in de applicatie log. Dat is de verklaring van regel één.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

De main task, die heeft volgens mij alleen een Start en geen Bind.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is een soort homepage. Op die andere schermen, volgens mij komt die Bind daar vandaan. Op het moment dat je een formulier op het schermt toont, moet de data uit de database gebind

Nummer: 1 Auteur: Persoonsgegevens Onderwerp: Opmerking over tekst Datum: 18-9-2020 11:30:21

'AB' moet zijn 'AD', en staat voor Active Directory

Persoonsgegevens

Ik zie hier use case staan, die heet aanpakken, klikmelding, task. Dat zou een voorbeeld kunnen zijn waar in ieder geval dat veld wordt aangeroepen. Het lijkt op een use case die daarmee te maken heeft.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is alleen het bewijs dat het scherm is aangeroepen, verder nog niks.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat zou ik verwachten.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Het is genoteerd.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Nee, dat is toen geannuleerd.

Persoonsgegevens

Dat kan ik uitsluiten, dat kan niet gelogd worden.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

We kunnen zien dat de export aangemaakt is, maar we kunnen niet zien dat die daadwerkelijk ergens opgeslagen is.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Nummer: 1 Auteur: Persoonsgegevens Onderwerp: Opmerking over tekst Datum: 18-9-2020 11:39:20

Persoonsgegevens moet vervangen worden door Persoonsgegevens

Persoonsgegevens

Nee, dat kun je ook niet zien.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Je hebt het nou over de kwaadwillende medewerker. Nogmaals, ik zal niet zeggen dat er geen kruit tegen gewassen is, maar je kan niet je organisatie beschermen tegen de kwaadwillende medewerker. Iemand die echt kwaad wil, zal kwaad doen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Per ongeluk is lastig, want per ongeluk kom je niet op internet bij ons. Dat is precies wat de heer Persoonsgegevens zegt. Wij hebben logging op de mail zitten. Als je bestanden naar buiten stuurt, dan wordt dat gelogd. Dat kunnen we altijd terugvinden. Dan is het niet per ongeluk gegaan. Dat is onder andere wat toentertijd het beruchte broedkameronderzoek ook aangetoond heeft. Daar waren ook bestanden opgeleverd aan een externe partij. Die hebben gewoon in logging terug kunnen vinden van hoe dat gebeurd is, welke bestanden dat waren en op welk moment dat was. Achteraf wel, maar voorkomen dat iemand vooraf heel bewust met informatie naar buiten gaat, dat is voor geen enkele organisatie te organiseren. Kijk naar mensen Persoonsgegevens wat die naar buiten brengt op een plek waarvan je niet verwacht dat het naar buiten gebracht kan worden. En als ik zie hoeveel geld zijn hebben voor beveiliging en hoeveel geld wij hebben als overheid voor beveiliging dan zit er énig verschil tussen. Ik heb niet de illusie dat wij onze medewerkers, de kwaadwillende medewerker echt kunnen tegenhouden. Wij gaan uit van het goede van de mens, en uiteraard nemen wij de mogelijke maatregelen die nodig zijn om de meeste opties uit te schakelen, maar het werk moet nog wel mogelijk zijn.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Je bedoelt het software-component wat wij gebruiken om te kunnen loggen, naar een textfile?

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Dat is [1]gfornet. Dat is een open source component die wij dit voor soort doeleinden gebruiken.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja. Die vragen wij dan op bij de functioneel beheerder.

Nummer: 1 Auteur: Persoonsgegevens Onderwerp: Opmerking over tekst Datum: 18-9-2020 11:43:58

formeel is het 'Log4Net'

Persoonsgegevens

De generieke tooling heet PAM tooling, Priviliged Acces management. Maar welke tool we daar als Belastingdienst voor gebruiken weet ik niet. Waarschijnlijk is die ook platform afhankelijk, want ik kan mij niet voorstellen dat er één tool bestaat die voor alle platforms die de Belastingdienst heeft.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Ja.

Persoonsgegevens

Een deel van die logging zoals de heer Persoonsgegevens schetst, dat herken ik wel maar dat is specifiek voor Windows sequel server ook zo geregeld dat die specifiek voor die database een wachtwoord krijgt. Volgens mij zit het in zijn profiel of rol dat hij bij de database mag, maar de toegang tot die database wordt absoluut gelogd en wat hij daarin doet ook.

Persoonsgegevens

Het kan zijn dat voor de sequel server die hier gebruikt wordt net een iets andere procedure geldt, maar het wordt standaard gelogd. Het zou niet best zijn als wij on-gelogd beheerders toegang tot systemen geven. Dat is voor de financiële stroom van belastingdienst niet verantwoordt. Als wij het niet kunnen garanderen hoe het geld tot stand gekomen is en de opbrengsten tot stand gekomen zijn, dan hebben wij een uitdaging.

Persoonsgegevens

Ik kom het in de praktijk in deze ook tegen van als je zegt 'kun je dat even voor mij uitvoeren', dat je dat alleen doet op basis van een opdracht. Je maakt een incident of een werkorder, dan wordt het gelogd en dan zit het in zijn proces. Dan heeft hij toestemming om bij die database te mogen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Die vraag kun je dan gewoon aan ons stellen.

Persoonsgegevens

Inspectie, controle en toezicht

Persoonsgegevens

Inspectie, controle en toezicht

Nummer: 1 Auteur: Persoonsgegevens Onderwerp: Opmerking over tekst Datum: 18-9-2020 11:51:26

Persoonsgegevens moet zijn Persoonsgegevens

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: dinsdag 29 september 2020 10:31
Aan: Persoonsgegevens
Onderwerp: RE: onderzoek FSV - reactie op Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

Dank u voor het nogmaals aanbieden. Ik heb zojuist het document *Verklaringen telefonisch afgelegd door Belastingdienst op 20 augustus 2020v-Opmerkingen-AvB.pdf* in goede orde ontvangen via de Bestandenpostbus.

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

'Privacy gaat iedereen wat aan'
De privacywet (AVG) zorgt voor meer grip op persoonsgegevens. Weten wat de privacywet voor jou betekent? Kijk op www.hulpbijprivacy.nl.

Van: Persoonsgegevens @minfin.nl>
Verzonden: dinsdag 29 september 2020 10:01
Aan: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Onderwerp: RE: onderzoek FSV - reactie op Aanlevering verklaringen logging 20 augustus 2020

Geachte mevrouw Persoonsgegevens

In reactie op uw bericht heb ik het bestand met de opmerkingen van de heer Persoonsgegevens nog een keer aangeboden via de bestandenpostbus. Het lijkt nu wel gelukt.

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

Van: Persoonsgegevens @minfin.nl>
Verzonden: dinsdag 13 oktober 2020 17:15
Aan: Persoonsgegevens
Onderwerp: Stukken FSV en 1043

Geachte mevrouw Persoonsgegevens

Hierbij de links naar de documenten over FSV, plan van aanpak FSV en

1-Lijst van vragen en antwoorden over o.a. informatie over de Fraude Signalering Voorziening (FSV) en het gebruik van FSV binnen de Belastingdienst (Kamerstuk 31066-681)

2-Concept plan van aanpak 'Herstellen, Verbeteren en Borgen'

3-Onderzoek naar projectcode 1043

,ittps://www.tweedekamer.nl/kamerstukken/detail?id=2020Z18727&did=2020D40520

https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z18725&did=2020D40511

https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z18731&did=2020D40540

Ik vertrouw erop u hiermee van dienst te zijn.

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

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: donderdag 15 oktober 2020 08:45
Aan: Persoonsgegevens
Onderwerp: RE: Stukken FSV en 1043

Geachte mevrouw Persoonsgegevens

Dank u voor het toesturen van de links naar de gepubliceerde stukken.

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

Van: Persoonsgegevens @minfin.nl>
Verzonden: dinsdag 13 oktober 2020 17:15
Aan: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Onderwerp: Stukken FSV en 1043

Geachte mevrouw Persoonsgegevens

Hierbij de links naar de documenten over FSV, plan van aanpak FSV en

1-Lijst van vragen en antwoorden over o.a. informatie over de Fraude Signalering Voorziening (FSV) en het gebruik van FSV binnen de Belastingdienst (Kamerstuk 31066-681)

2-Concept plan van aanpak 'Herstellen, Verbeteren en Borgen'

3-Onderzoek naar projectcode 1043

https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z18727&did=2020D40520

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: vrijdag 23 oktober 2020 15:17
Aan: Persoonsgegevens
Onderwerp: Onderzoek FSV: informatieverzoek autorisaties FSV

Hierbij nogmaals de mail maar dan zonder opmaak, hopelijk is deze wel goed te lezen.

Geachte mevrouw Persoonsgegevens

Tijdens het Onderzoek ter Plaatse (OTP) op 30 juni 2020 zijn er door de Belastingdienst verklaringen afgelegd over de inrichting van de autorisaties voor de FSV-applicatie. Daarnaast bevatten de tot nu toe overlegde documenten bepaalde informatie over de inrichting van de autorisaties. Bij de bestudering van de afgelegde verklaringen en deze documenten zijn nadere vragen gerezen over dit onderwerp.

:rzoeken om informatie
.en behoeve van het onderzoek verzoek ik u antwoord te geven op de volgende vragen. Dit betreft een verzoek om informatie als bedoeld in artikel 58, eerste lid, onder a AVG en de artikelen 5:16 Algemene wet bestuursrecht (Awb) jo. 5:17 Awb. U bent niet verplicht te antwoorden op de vragen. Voor wat betreft het verstrekken van documenten bent u op grond van artikel 31 AVG en artikel 5:20 Awb wel verplicht tot medewerking.

Vragen
1. In paragraaf 2.3.1 van het onderzoeksrapport van de ADR getiteld 'Implementatie AVG bij het Ministerie van Financiën' van 10 april 2019 met kenmerk 2019-000062907 is beschreven dat alle dienstonderdelen van de Belastingdienst vóór 1 oktober 2018 moesten rapporteren over de actualiteit van hun autorisaties. De AP verzoekt u om deze rapportages en andere relevante documentatie te verstrekken.
2. Tijdens het OTP is door de plaatsvervangend CISO verklaart dat directies periodiek de toegekende autorisaties in IMS controleren en dat dit (hopelijk) is vastgelegd omdat de ADR daarop controleert (p. 82 van het verslag). De AP verzoekt u om een lijst op te stellen met alle beoordelingen van de voor FSV afgegeven autorisaties die hebben plaatsgevonden in de jaren dat de FSV-applicatie werd gebruikt (2013-februari 2020). Ik doel hierbij zowel op periodiek uitgevoerde beoordelingen als op beoordelingen die incidenteel zijn uitgevoerd. Ik verzoek u in de lijst per beoordeling de volgende informatie aan te leveren:
   a. De aanleiding voor de beoordeling;
   b. De datum waarop de autorisaties zijn beoordeeld;
   c. Door wie/welke directie de beoordeling is uitgevoerd;
   d. Of en zo ja welke handleiding c.q. specifieke instructies er zijn meegegeven;
   e. Of en zo ja welke informatie beschikbaar werd gesteld ter ondersteuning van de beoordeling (bijvoorbeeld een IMS Rollenplaat van een dienstonderdeel)
   f. De resultaten van de beoordeling voor de autorisaties van FSV;
   g. Het gevolg van de beoordeling voor de autorisaties van FSV.
3. De AP verzoekt u de handleidingen en specifieke instructies (sub d in vraag 2), de ondersteunende informatie (sub e in vraag 2) en de resultaten van de beoordeling (sub f in vraag 2) en alle overige relevante documentatie van elke beoordeling te verstrekken.
4. De AP verzoekt u toe te lichten of er in de periode 2013 – februari 2020 binnen de Belastingdienst een procedure was voor het periodiek beoordelen van de uitgegeven autorisaties. De AP verzoekt u deze procedure(s) te verstrekken.

Termijn
De AP verzoekt u de gevraagde informatie in vraag 1 uiterlijk vrijdag 30 oktober aan te leveren en de gevraagde informatie in vraag 2, 3 en 4 uiterlijk vrijdag 6 november 2020. De informatie kan worden verstrekt via de Bestandenpostbus.

Afschrift
Een afschrift van dit verzoek om informatie is per e-mail aan uw functionaris voor de gegevensbescherming gestuurd: fg@minfin.nl is opgenomen in de cc.

Indien u vragen heeft over dit verzoek om informatie, kunt u contact opnemen met onderstaande contactpersoon.

Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: vrijdag 23 oktober 2020 15:19
Aan: Persoonsgegevens
Onderwerp: RE: Onderzoek FSV: informatieverzoek autorisaties FSV

Geachte mevrouw Persoonsgegevens

Dank voor het nogmaals sturen van het bericht.

Deze versie is goed leesbaar.

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

Van: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Verzonden: vrijdag 23 oktober 2020 15:17
Aan: Persoonsgegevens @minfin.nl>
Onderwerp: Onderzoek FSV: informatieverzoek autorisaties FSV

Hierbij nogmaals de mail maar dan zonder opmaak, hopelijk is deze wel goed te lezen.

Geachte mevrouw Persoonsgegevens

Tijdens het Onderzoek ter Plaatse (OTP) op 30 juni 2020 zijn er door de Belastingdienst verklaringen afgelegd over de inrichting van de autorisaties voor de FSV-applicatie. Daarnaast bevatten de tot nu toe overlegde documenten bepaalde informatie over de inrichting van de autorisaties. Bij de bestudering van de afgelegde verklaringen en deze documenten zijn nadere vragen gerezen over dit onderwerp.

Verzoeken om informatie
Ten behoeve van het onderzoek verzoek ik u antwoord te geven op de volgende vragen. Dit betreft een verzoek om informatie als bedoeld in artikel 58, eerste lid, onder a AVG en de artikelen 5:16 Algemene wet bestuursrecht (Awb) jo. 5:17 Awb. U bent niet verplicht te antwoorden op de vragen. Voor wat betreft het verstrekken van documenten bent u op grond van artikel 31 AVG en artikel 5:20 Awb wel verplicht tot medewerking.

Vragen
1. In paragraaf 2.3.1 van het onderzoeksrapport van de ADR getiteld 'Implementatie AVG bij het Ministerie van Financiën' van 10 april 2019 met kenmerk 2019-000062907 is beschreven dat alle dienstonderdelen van de Belastingdienst vóór 1 oktober 2018 moesten rapporteren over de actualiteit van hun autorisaties. De AP verzoekt u om deze rapportages en andere relevante documentatie te verstrekken.

Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: dinsdag 27 oktober 2020 09:09
Aan: Persoonsgegevens
Onderwerp: RE: Onderzoek FSV: informatieverzoek autorisaties FSV

Geachte mevrouw Persoonsgegevens

Naar aanleiding van onderstaande vragen, zou ik graag nader willen overleggen.

Kunt u aangeven wanneer u beschikbaar bent?

Bij voorbaat dank voor uw reactie.

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

Van: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Verzonden: vrijdag 23 oktober 2020 15:17
Aan: Persoonsgegevens @minfin.nl>
Onderwerp: Onderzoek FSV: informatieverzoek autorisaties FSV

:rbij nogmaals de mail maar dan zonder opmaak, hopelijk is deze wel goed te lezen.

Geachte mevrouw Persoonsgegevens

Tijdens het Onderzoek ter Plaatse (OTP) op 30 juni 2020 zijn er door de Belastingdienst verklaringen afgelegd over de inrichting van de autorisaties voor de FSV-applicatie. Daarnaast bevatten de tot nu toe overlegde documenten bepaalde informatie over de inrichting van de autorisaties. Bij de bestudering van de afgelegde verklaringen en deze documenten zijn nadere vragen gerezen over dit onderwerp.

Verzoeken om informatie
Ten behoeve van het onderzoek verzoek ik u antwoord te geven op de volgende vragen. Dit betreft een verzoek om informatie als bedoeld in artikel 58, eerste lid, onder a AVG en de artikelen 5:16 Algemene wet bestuursrecht (Awb) jo. 5:17 Awb. U bent niet verplicht te antwoorden op de vragen. Voor wat betreft het verstrekken van documenten bent u op grond van artikel 31 AVG en artikel 5:20 Awb wel verplicht tot medewerking.

Vragen
1. In paragraaf 2.3.1 van het onderzoeksrapport van de ADR getiteld 'Implementatie AVG bij het Ministerie van Financiën' van 10 april 2019 met kenmerk 2019-000062907 is beschreven dat alle dienstonderdelen van de

110.

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: dinsdag 27 oktober 2020 10:08
Aan: Persoonsgegevens
Onderwerp: RE: Onderzoek FSV: informatieverzoek autorisaties FSV

Geachte mevrouw Persoonsgegevens

Ik heb u zojuist telefonisch gesproken, waarbij u een aantal vragen had over het informatieverzoek over autorisaties FSV. Hierbij koppel ik kort terug wat wij zojuist hebben gesproken en noteer ik de gemaakte afspraken:

Over vraag 1:
U heeft toegelicht dat u van uw collega dhr Persoonsgegevens een aantal Excel-bestanden heeft ontvangen met daarin een aantal vaste vragen die elke directie moest beantwoorden. De vragenlijst ging over de implementatie van de AVG als geheel, en ging dus verder dan alleen het aspect autorisaties. U heeft toegelicht dat dit de eindrapportages lijken te zijn van de implementatie van de AVG binnen de BD in het jaar na 25 mei 2018 (NB: de Belastingdienst had destijds ansparant naar buiten gecommuniceerd dat zij op 25 mei 2018 nog niet AVG-proof was maar hiervoor nog een jaar odig had).

De Excel-bestanden met de eindrapportages lijken uit juli 2019 te zijn. In ons gesprek hebben we daarom geconcludeerd dat dit niet de door de AP opgevraagde rapportages zijn die alle dienstonderdelen voor 1 oktober 2018 moesten opleveren over de afgegeven autorisaties (zie paragraaf 2.3.1 van het ADR rapport van 10 april 2019 https://www.rijksoverheid.nl/documenten/rapporten/2019/05/28/rapport-adr-over-implementatie-avg-bij-financien).

De Excelbestanden met de eindrapportages kwalificeren wel als 'andere relevante informatie' zoals genoemd in vraag 1. De AP gaf aan het goed te vinden als de BD uit deze eindrapportages allen de informatie over de autorisaties knipt en deze aanlevert aan de AP.
Afspraken:

- De BD gaat op zoek naar de rapportages zijn die alle dienstonderdelen voor 1 oktober 2018 moesten aanleveren over autorisaties en levert deze alsnog aan.
- De BD knipt alleen de informatie over de autorisaties uit de Excel eindrapportages en levert dit aan de AP aan.

Over vraag 2:
U gaf aan dat dhr Persoonsgegevens vraag 2 heeft uitgelegd dat de controle van de autorisaties op rolniveau plaatsvond en dat het voor manager niet inzichtelijk is welke autorisaties tot welke applicaties er in een rol zitten. De AP heeft hierop gereageerd door te zeggen dat dit is wat dhr Persoonsgegevens ons het OTP heeft verklaard. Dit doet niet af aan de vragen die de AP heeft gesteld.
U legt uit dat in 2018 het huidige IMS rollenmodel is geïmplementeerd en u vraagt zich af of de AP ook op zoek is naar de informatie voor deze implementatie, want dit zou dan per dienstonderdeel moeten worden opgevraagd (ofwel de informatie is lastiger boven water te krijgen).
Afspraken:

- De BD gaat na wanneer precies het huidige IMS rollenmodel is geïmplementeerd en wat de aanleiding was.
- De BD levert voor nu alleen de gevraagde informatie op na implementatie van het huidige IMS rollenmodel.
- De AP komt later deze week terug op de vraag (afhankelijk van het antwoord op de eerste afspraak over wanneer IMS is geïmplementeerd in 2018) of de informatie ook van voor 2018 moet worden opgeleverd door de BD.

Ik hoop dat ik hetgeen we hebben besproken en de gemaakte afspraken zo juist geformuleerd heb.

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

'Privacy gaat iedereen wat aan'
De privacywet (AVG) zorgt voor meer grip op persoonsgegevens. Weten wat de privacywet voor jou betekent? Kijk op www.hulpbijprivacy.nl.

Van: Persoonsgegevens @minfin.nl>
Verzonden: dinsdag 27 oktober 2020 09:09
Aan: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Onderwerp: RE: Onderzoek FSV: informatieverzoek autorisaties FSV

Geachte mevrouw Persoonsgegevens

Naar aanleiding van onderstaande vragen, zou ik graag nader willen overleggen.

Kunt u aangeven wanneer u beschikbaar bent?

Bij voorbaat dank voor uw reactie.

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

Van: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Verzonden: vrijdag 23 oktober 2020 15:17
Aan: Persoonsgegevens @minfin.nl>
Onderwerp: Onderzoek FSV: informatieverzoek autorisaties FSV

Hierbij nogmaals de mail maar dan zonder opmaak, hopelijk is deze wel goed te lezen.

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: maandag 2 november 2020 12:18
Aan: Persoonsgegevens
CC: 'fg@minfin.nl'
Onderwerp: RE: Onderzoek FSV: informatieverzoek autorisaties FSV

Geachte mevrouw Persoonsgegevens

Ik heb u zojuist telefonisch gesproken over het informatieverzoek dat de Autoriteit persoonsgegevens (AP) op vrijdag 23 oktober 2020 aan de Belastingdienst heeft gedaan. Afgelopen vrijdag verliep de deadline voor het antwoord op vraag 1 en omdat ik van u nog geen reactie had ontvangen heb ik u gebeld. U gaf aan dat de Belastingdienst de verzochte informatie niet zal aanleveren.

We hebben zojuist telefonisch afgesproken dat de Belastingdienst met een schriftelijke reactie komt waarom de informatie niet kan worden aangeleverd. De AP verzoekt de Belastingdienst om gedetailleerd aan te geven:

(1) welke van de gevraagde informatie niet kan worden aangeleverd, daarbij refererend aan onderstaande e-mails (het informatieverzoek van 23 oktober en de nadere afspraken van 27 oktober);
(2) de precieze reden voor het niet aanleveren;
(3) welke informatie wel zal worden aangeleverd en of dit binnen de gestelde termijn (uiterlijk 6 november 2020) gaat plaatsvinden.

Een kopie van deze mail is tevens verzonden aan de FG van de Belastingdienst.

Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

'Privacy gaat iedereen wat aan'
De privacywet (AVG) zorgt voor meer grip op persoonsgegevens. Weten wat de privacywet voor jou betekent? Kijk op www.hulpbijprivacy.nl.

Van: Persoonsgegevens
Verzonden: dinsdag 27 oktober 2020 10:08
Aan: Persoonsgegevens @minfin.nl>
Onderwerp: RE: Onderzoek FSV: informatieverzoek autorisaties FSV

Persoonsgegevens

Van: Persoonsgegevens
Verzonden: vrijdag 6 november 2020 09:09
Aan: Persoonsgegevens
Onderwerp: Mogelijkheden gesprek in onderzoek FSV

Geachte mevrouw Persoonsgegevens

Afgelopen woensdag spraken wij elkaar over de informatie die u namens de Belastingdienst gaat aanleveren als reactie op het informatieverzoek van 23 oktober 2020 aangaande autorisaties. In het telefoongesprek gaf u aan dat de Belastingdienst mogelijk een verzoek zou gaan doen voor een gesprek om de overlegde informatie mondeling toe te lichten. Graag leg ik hierbij uit hoe zo een gesprek in een onderzoek als de onderhavige eruit zou zien.

Eind februari 2020 kwam via de media een GEB naar buiten over de binnen de Belastingdienst gebruikte Fraude Signalering Voorziening (FSV). De GEB stelde dat de FSV-applicatie op meerdere onderdelen in strijd was met de AVG. De Staatssecretarissen hebben dit in hun brieven aan de Tweede Kamer herhaald. Dit was voor de AP aanleiding om een onderzoek te starten. Dit betreft een onderzoek met het oog op handhaving.

In een onderzoek met het oog op handhaving is het essentieel dat elk bewijsstuk zorgvuldig wordt vastgelegd en in het dossier komt. Er is geen ruimte voor informele uitwisselingen van informatie, omdat in het rapport geen informatie gebruikt kan worden die niet in het dossier zit. Een verzoek om een mondelinge toelichting betekent dus dat u verzoekt om verhoord te worden door de AP. Dit betekent concreet: een call via videoverbinding, het verhoor zal worden opgenomen, schriftelijk worden uitgewerkt, aan de Belastingdienst worden voorgelegd voor controle en tot slot wordt het document opgenomen in het dossier. Daarbij is het ook zo dat de AP bepaald wie zij verhoord.

Het staat de Belastingdienst vrij om een verzoek tot een verhoor te doen. Ik hoop wel dat u begrijpt dat gezien de tijd en moeite die het kost om dit verhoor vast te leggen dat de AP dit verzoek alleen zal inwilligen als zij inschat dat dit echt nodig is. Ik wil u dan ook vriendelijk verzoeken om de schriftelijke informatie die u later vandaag namens de Belastingdienst gaat indienen zo volledig mogelijk te laten zijn en niet ervan uit te gaan dat er een verhoor zal plaatsvinden.

Ik hoop u hiermee voldoende geïnformeerd te hebben.

et vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bezoekadres: Bezuidenhoutseweg 30, 2594 AV Den Haag
Postadres: Postbus 93374, 2509 AJ Den Haag
www.autoriteitpersoonsgegevens.nl

'Privacy gaat iedereen wat aan'

Persoonsgegevens

Van: Persoonsgegevens @minfin.nl>
Verzonden: vrijdag 6 november 2020 20:51
Aan: Persoonsgegevens
Onderwerp: z2020-04615 - Onderzoek FSV: informatieverzoek autorisaties FSV

Geachte mevrouw Persoonsgegevens

Hierbij stuur ik u de reactie van de Belastingdienst op uw verzoek van 23 oktober 2020. Ik betreur dat het niet gelukt is om -conform de wens van de AP- per 30 oktober 2020 te reageren op het eerste deel van uw verzoek. Dit had niet mogen gebeuren en ik bied u hiervoor mijn verontschuldigingen aan.

De Belastingdienst wil graag zo goed mogelijk aan de verzoeken van de AP voldoen en zal daarom de beschikbare documenten integraal verstrekken. De Belastingdienst realiseert zich dat de gegevens die nu aan de AP verstrekt worden, mogelijk mager zijn en niet voldoen aan de verwachtingen van de AP. Voor sommige onderdelen is het echter moeilijk de gevraagde documenten aan te leveren. Om die reden stelt de Belastingdienst voor een extra gesprek in te plannen. Aan de hand van dat gesprek kan de beschikbare informatie worden geleverd, dan wel worden gemotiveerd waarom de informatie er niet beschikbaar is in de vorm die de AP vraagt.

De Belastingdienst is zich ervan bewust dat een extra gesprek ook zorgt voor extra werklast en effect heeft voor de voortgang van het onderzoek van de AP. De Belastingdienst zal zich inspannen om een gesprek zo veel mogelijk te faciliteren, opdat de extra belasting voor de AP zo min mogelijk zal zijn.

Via de concerndirecteur Persoonsgegevens heb ik vernomen dat de AP nog wacht op reacties op verzoeken van 24 en 30 juli 2020. Aangezien de verzoeken ook zien op autorisaties, kunnen deze wellicht ook in het voorgestelde extra gesprek behandeld worden.

Voor het (vervolg)gesprek c.q. verhoor wordt gedacht met de volgende personen:
Persoonsgegevens
Persoonsgegevens welk onderdeel verantwoordelijk is voor het logisch toegangsbeheer; en
Persoonsgegevens die verantwoordelijke is voor de applicatie FSV.

Vraag 1 - rapporteren over de actualiteit van autorisaties
In het zip-bestand (aangeboden via de bestandenpostbus) vindt u per directie de eindrapportage zoals besproken in het MT DT van juni 2019. Rapportages bevatten dus meer dan alleen het antwoord op de vraag over de actualiteit van de autorisaties. Overigens hebben de meeste directies aangegeven dat actualiseren per 18 oktober 2018 niet realiseerbaar was. Per mei 2019 hebben alle directeuren aangegeven dat ze de actie afgerond hebben.

De status van de actie "autorisaties op orde" kan voor iedere directie een ander volgnummer hebben. Voor het juiste beeld kan de AP zoeken op de term "autorisaties" in de betreffende kolom.

Daarnaast stuur ik u als andere relevante documentatie de '180717 notitie DT beleidslijnen en acties AVG geconsolideerd' en het 'eindrapport programma AVG'.

De documenten zijn aangeboden via de bestandenpostbus.

Vraag 2 – beoordelingen autorisaties FSV
De Belastingdienst stelt voor om voor de beantwoording van deze vraag eerst een aanvullende gesprek te houden.

Vraag 3 - handleidingen en specifieke instructies
De handleidingen voor FSV en specifieke instructies zijn reeds openbaar. Deze zijn gepubliceerd bij de brief aan de Kamer van 10 juli 2020. Een link naar deze brief is op 10 juli 2020 aan de AP gestuurd.

Gestuurde link: https://www.rijksoverheid.nl/documenten/kamerstukken/2020/07/10/aanbiedingsbrief-fsv
Alternatieve link: https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z13850&did=2020D29414

Vraag 4 – procedures periodiek beoordelen autorisaties
De Belastingdienst stelt voor om voor de beantwoording van deze vraag eerst een aanvullende gesprek te houden.

Graag verneem ik of de AP in de gelegenheid is om een extra gesprek te hebben met de Belastingdienst.

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

Van: Persoonsgegevens @autoriteitpersoonsgegevens.nl>
Verzonden: maandag 2 november 2020 12:18
Aan: Persoonsgegevens @minfin.nl>
CC: FG@minfin.nl
Onderwerp: RE: Onderzoek FSV: informatieverzoek autorisaties FSV

Geachte mevrouw Persoonsgegevens

Ik heb u zojuist telefonisch gesproken over het informatieverzoek dat de Autoriteit persoonsgegevens (AP) op vrijdag 23 oktober 2020 aan de Belastingdienst heeft gedaan. Afgelopen vrijdag verliep de deadline voor het antwoord op vraag 1 en omdat ik van u nog geen reactie had ontvangen heb ik u gebeld. U gaf aan dat de Belastingdienst de verzochte informatie niet zal aanleveren.

We hebben zojuist telefonisch afgesproken dat de Belastingdienst met een schriftelijke reactie komt waarom de informatie niet kan worden aangeleverd. De AP verzoekt de Belastingdienst om gedetailleerd aan te geven:
(1) welke van de gevraagde informatie niet kan worden aangeleverd, daarbij refererend aan onderstaande e-mails (het informatieverzoek van 23 oktober en de nadere afspraken van 27 oktober);
(2) de precieze reden voor het niet aanleveren;
(3) welke informatie wel zal worden aangeleverd en of dit binnen de gestelde termijn (uiterlijk 6 november 2020) gaat plaatsvinden.

Een kopie van deze mail is tevens verzonden aan de FG van de Belastingdienst.
Met vriendelijke groet,

Persoonsgegevens
Senior juridisch medewerker

AUTORITEIT
PERSOONSGEGEVENS

Kantoor: 070 8888 500
Persoonsgegevens
Fax: 070 8888 501

Bylage 1

Ministerie van Financiën

TER BESPREKING
Aan:
Directieteam Belastingdienst

Geconsolideerde versie naar aanleiding van bespreking en aanvullende notities in de DT's van 18 mei, 7 juni en 5 juli 2018, en op basis van rapportage aan de Bestuursraad MinFin van 13 juni 2018

Directoraat-Generaal
Belastingdienst

Persoonsgegevens

Datum
juli 2018

Notitienummer

Auteur

Van

Bijlagen

notitie

AVG: beleidslijnen en acties naar aanleiding van inventarisatie en risicoanalyse gegevensverwerkingen

1. Inleiding

Op de gegevensverwerkingen die zijn geïnventariseerd ten behoeve van opneming in het AVG-register is een risico- en issueanalyse uitgevoerd om te bepalen waar op korte en langere termijn maatregelen zijn om de naleving van de AVG te verbeteren.
De rapportages met de risico's en issues en de daarop te nemen maatregelen zijn door de inventarisatieteams opgeleverd aan de (keten)directeur of proceseigenaar. Deze is verantwoordelijk voor de realisatie van de maatregelen. De rapportages worden behandeld in de ketenportfolioboards en in het bedrijfsvoeringsportfolio-overleg, zodat waar nodig de consequenties in de IV-portfolio kunnen worden doorgevoerd en prioriteiten kunnen worden gesteld. De maatregelen moeten voorts onderdeel worden van de jaarplannen van de desbetreffende directies en van de reguliere verantwoording daarover door de desbetreffende directeur aan de DG. De Ketentafel gegevens kan een ondersteunende rol spelen in de bewaking van de voortgang.

Het bepalen de mate van compliance die met de te nemen maatregelen bereikt wordt, vereist een norm waaraan getoetst kan worden. De AVG bevat veel open normen, die ruimte laten voor interpretatie. In paragraaf 3.1 zijn de deze open normen beschreven. Mede op grond van de in kaart gebrachte risico's en issues wordt ten aanzien van de open normen een *beleidslijn* geformuleerd of wordt een voorstel gedaan om daartoe te komen (*actie*).
De AVG bevat ook een aantal gesloten normen met concrete verplichtingen. Deze zijn opgenomen in paragraaf 3.2. Daarbij is (mede op grond van de genoemde rapportages) een aantal meer generieke risico's en issues vermeld en worden de maatregelen voorgesteld om deze op afzienbare termijn weg te nemen (*acties*).

De beleidslijnen gelden concernbreed, dus voor alle dienstonderdelen. Door deze beleidslijnen vast te stellen en te zorgen dat alle onderdelen in overeenstemming daarmee opereren, kan de Belastingdienst een afdoende niveau van voldoening aan de AVG verantwoorden.
Uitvoering van de maatregelen in de risicorapportages en van de in deze notitie beschreven acties is noodzakelijk voor het binnen de beleidslijnen opereren, en dus voor compliantie met de AVG; het binnen de genoemde termijnen uitvoeren van die acties is dan ook noodzakelijk. Een oordeel van de AP of de rechter over

een bepaalde handelwijze kan uiteraard invloed hebben op het nalevingsniveau. Dat kan wijziging of aanvulling van de beleidslijnen en acties nodig maken.

Uit de rapportages komen drie issues naar voren die Belastingdienstbreed spelen en die met voorrang actie vereisen, omdat ze de belangrijkste nalevingsrisico's opleveren. Dit zijn:

- *Schonen van systemen en gegevensbestanden*
  Vrijwel overal is achterstand in het vernietigen van (persoons)gegevens in systemen en bestanden op basis van de vastgestelde selectielijsten. Ook wordt nog veel niet-archiefwaardig materiaal bewaard (inclusief persoonsgegevens) dat niet meer nodig is voor het werk.

- *Delen van gegevens*
  - intern: er wordt veel gebruik gemaakt van faciliteiten voor het delen van gegevens, waardoor het risico bestaat van ongebreideld (her)gebruik en te brede toegang tot gegevens. Voorbeelden zijn applicaties als Wisselland, LOA's met personeelsgegevens, datadumpingfaciliteiten.
  - extern: er is een aantal verstrekkingen aan externe partijen waarvoor de grondslag niet bekend of duidelijk is. Andere risicovolle verwerking is het gebruik van BSN's uit de personeelsadministratie voor de zogenoemde ambtenarentabel.

- *Autorisaties*
  Toegang tot persoonsgegevens is gebaseerd op taken en functies, met als uitgangspunten zijn integrale klantbehandeling en landelijke inzet. Dit leidt tot vrij ruime autorisaties. Dat hoeft (mede gelet op de brede doelbinding) geen probleem te zijn, maar het vraagt wel zorgvuldig beheer. Op dat punt is sowieso verbetering nodig, en verder kan meer gebruik gemaakt worden van mogelijkheden die de techniek biedt om te differentiëren in toegang, op basis van aard, gebruik en gebruikers van de gegevens.

Over een aantal punten in paragraaf 3 zijn al eerder besluiten genomen in het DT. Deze besluiten zijn bij het desbetreffende onderwerp herhaald, met vermelding van de datum van het DT waarin deze genomen zijn.

2. Relatie met privacybeleid Financiën

Het Ministerie van Financiën heeft een privacybeleid vastgesteld. Daarin zijn de kaders voor omgaan met (persoons)gegevens opgenomen en is de governance uitgewerkt (oa. het beleggen van de rollen van CIO, CISO, privacy officer en datacoördinator en de plaats van de FG in dit geheel). Het privacybeleid laat uitdrukkelijk ruimte voor invulling door de onderdelen van het ministerie, zowel wat betreft beleid als wat betreft governance.

Met vaststelling van het advies voor inrichting van de privacyfunctie en de inrichting van de Concerndirectie IV&D (waar de rollen van CIO, CDO, CSO en CISO zijn belegd), wordt uitwerking gegeven aan de governance bij de Belastingdienst. Ter invulling van de privacyfunctie wordt bij de onderdelen op dit moment de rol van datacoördinator vervuld.

Met de beleidslijnen die in deze notitie zijn opgenomen, wordt het privacybeleid voor de Belastingdienst verder uitgewerkt.

3. Open en gesloten normen in de AVG

De AVG benoemt in artikel 5 een aantal beginselen voor bescherming van persoonsgegevens. Dit zijn

- Rechtmatigheid, behoorlijkheid en transparantie
- Doelbinding
- Minimale gegevensverwerking
- Juistheid
- Opslagbeperking
- Integriteit en vertrouwelijkheid
- Verantwoordingsplicht

Deze beginselen zijn vrijwel alle in verschillende artikelen van de AVG uitgewerkt, ofwel in open normen, ofwel in gesloten normen (concrete verplichtingen).

Een essentiële bepaling in de AVG is artikel 24, dat een zeer algemene verplichting bevat tot naleving van de AVG, en een invulling van de *verantwoordingsplicht* over die naleving. Het vereist dat, rekening houdend met de aard, omvang, context en doel van de verwerking en de risico's voor betrokkenen die hieraan verbonden zijn, passende technische en organisatorische maatregelen worden getroffen om de verwerkingen in overeenstemming met de AVG uit te voeren en dat ook te kunnen aantonen. De genomen maatregelen moeten worden geëvalueerd en geactualiseerd.

Bij de Belastingdienst ligt de verantwoordelijkheid voor naleving van de AVG bij de dienstonderdelen. Het treffen van de benodigde maatregelen om verantwoord met (persoons)gegevens om te gaan vereist beleidslijnen en acties ten aanzien van de normen in de AVG. In het onderstaande worden de toepasselijke bepalingen uit de AVG besproken, voorzien van een beleidsstandpunt ten aanzien van de interpretatie en/of toepassing.

Het aantonen van (de werking van) genomen maatregelen is een continu proces, dat onderdeel uitmaakt van integraal datamanagement in de organisatie. Op een aantal terreinen ((informatie)beveiliging, IV) bestaan al mechanismen hiervoor, zoals KPI's in jaarcontracten, self assessments op informatiebeveiliging en audits. Ook PIA's op bestaande en nieuwe verwerkingen moeten hier inzicht in geven. Het ligt voor de hand om deze procedures te benutten om te voldoen aan deze bepaling.

3.1 Open normen

3.1.1 Opslagbeperking

Artikel 89 van de AVG bepaalt dat passende waarborgen in de vorm van technische en organisatorische maatregelen moeten worden getroffen om bij archivering in het algemeen belang, het beginsel van minimale gegevensverwerking te garanderen. Dit artikel vormt ook de uitwerking van het beginsel van *opslagbeperking* in artikel 5, eerste lid, onderdeel g, van de AVG. De Archiefwet en de op grond daarvan vastgestelde selectielijsten bieden het kader voor het bewaren of vernietigen van archiefwaardige gegevens en documenten. Uit de inventarisatie van gegevensverwerkingen blijkt dat voor alle verwerkingen selectielijsten bestaan en dus bewaar- cq. vernietigingstermijnen zijn vastgelegd. Actualiseren van deze selectielijsten, als onderdeel van regulier beheer, is noodzakelijk en is op initiatief van sso CFD ter hand genomen.

Voor niet-archiefwaardige bestanden (die ook persoonsgegevens kunnen bevatten; te denken valt aan bestanden in mailapplicaties, in samenwerkingsgebieden en op ConnectPeople) geldt het uitgangspunt dat zij vernietigd moeten worden zodra ze niet meer nodig zijn voor het werk.

Bestaande bestanden moeten uiterlijk eind 2018 worden geschoond aan de hand van de selectielijsten; dat betekent ofwel vernietiging van de bestanden, ofwel overbrenging naar het archief. Daarnaast worden uitkomsten van instrumenten zoals data discovery dashboards en de AVG-scan aan de Ketentafel gegevens aangeboden om concrete schoningsacties af te spreken en te bewaken.
Waar schoning niet automatisch kan plaatsvinden, moet dit periodiek handmatig worden herhaald. Deze acties worden geïnitieerd en bewaakt via de Ketentafel gegevens (wat de eigen verantwoordelijkheid van de onderdelen voor deze acties overigens onverlet laat).
In nieuwe systemen moeten voorzieningen voor automatisch schonen worden ingebouwd (dit is ook een maatregel in het licht van *privacy by design* en *by default*, zie hierna). Daarnaast moet in nieuwe voorzieningen ook een koppeling worden gerealiseerd met de generieke archiefvoorziening, zodat overbrenging van te bewaren bestanden automatisch kan plaatsvinden. Dit onwerpprincipe is al opgenomen in de referentiearchitectuur document- en archiefbeheer, die onderdeel uitmaakt van de concernarchitectuur.

In het beleid ten aanzien van schonen van persoonsgegevens moet specifieke aandacht worden besteed aan het ketenaspect: als de brongegevens en een eindproduct van gebruik van die gegevens bewaard blijven, moeten of mogen tussenbestanden dan nog bewaard worden? De bevindingen van de taskforce datahygiëne kunnen behulpzaam zijn bij uitwerking van dit aspect

De vernietigingstermijn voor persoonsgegevens die worden verwerkt in het kader van primaire en secundaire processen is afgestemd op de termijn waarbinnen nog acties op grond van deze gegevens nodig kunnen zijn. De eis dat persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkene niet langer de te identificeren dan nodig is voor het doel waarvoor de gegevens worden verwerkt, kan voor de Belastingdienst zo worden geïnterpreteerd dat op bewaarde gegevens geen nadere maatregelen nodig zijn, omdat gedurende de bewaartermijn altijd identificatie van de betrokkene nodig is in het licht van de wettelijke taken en bevoegdheden van de Belastingdienst.

Beslispunten

Beleidslijnen
a. Mede uit oogpunt van opslagbeperking van persoonsgegevens worden niet-archiefwaardige bestanden vernietigd zodra zij niet meer nodig zijn voor het werk.
b. Er worden geen nadere maatregelen getroffen om gearchiveerde bestanden te anonimiseren, omdat gedurende de bewaartermijn de daarin opgenomen persoonsgegevens noodzakelijk zijn voor de uitvoering van wettelijke taken.

Actie
c. Alle dienstonderdelen schonen uiterlijk eind 2018 bestaande gegevensbestanden op grond van de geldende selectielijsten; niet-archiefwaardige bestanden worden vernietigd, archiefwaardige bestanden worden overgebracht naar een archiefvoorziening. De voortgang van deze actie wordt bewaakt via de Ketentafel gegevens en sso CFD verleent hierbij ondersteuning.

3.1.2 Doelbinding en verdere verwerking
Artikel 6, vierde lid, regelt dat gegevens die voor een bepaald doel verzameld zijn, verder verwerkt mogen worden voor een doel dat daarmee verenigbaar is. Het is een uitzondering op het beginsel van *doelbinding*: persoonsgegevens worden alleen verwerkt voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. Als verder verwerkt wordt voor een verenigbaar doel, moet rekening gehouden worden met de belangen van de betrokkenen.

De doelen waarvoor de Belastingdienst gegevens verwerkt vloeien voort uit de wettelijke taken: heffen, uitkeren, innen, uitoefenen van goederentoezicht en opsporing van delicten.[1] Gebruik van voor deze doelen verzamelde de gegevens ten behoeve van toezicht, dienstverlening of communicatie, bijvoorbeeld door het bundelen van gegevensverzamelingen voor analytics of door ze contra-informatie beschikbaar te stellen in de VIA), kan aangemerkt worden als verwerking voor een verenigbaar doel.
De eis van doelbinding is onder de AVG niet anders dan onder de Wbp, wat het handhaven van deze invulling voor de Belastingdienst rechtvaardigt. Dat betekent dat gegevens 'over middelen heen' gebruikt kunnen blijven worden en dat ook de uitwisseling tussen belastingen en toeslagen (die overigens een eigen wettelijke grondslag kent in de Awir) mogelijk blijft. Daarbij kan het wel nodig of wenselijk zijn om te differentiëren naar gelang het gebruik van de gegevens (regulier gebruik, POC's, laboratoriumsetting) en de gebruikers (toegang voor iedereen, voor een bepaalde groep, of alleen voor de zaaksbehandelaar). De technische en organisatorische maatregelen die hiervoor genomen moeten worden, behoren tot het domein van de informatiebeveiliging (zie ook onderdeel 3.1.8).
Er ligt overigens wel druk op het meer preciseren van de doelbinding. Zo wordt in de Wet op de motorrijtuigenbelasting mede naar aanleiding van de rechterlijke uitspraken over ANPR-camerabeelden een concrete grondslag opgenomen voor gebruik van deze beelden, die uitdrukkelijk beperkt wordt tot gebruik voor heffing van de MRB. DGFZ werkt ook aan een wetsvoorstel gegevensgebruik Belastingdienst dat strakker zal reguleren op doelbinding (via amvb's waarin gegevensgebruik wordt uitgewerkt). Daarbij zal steeds bezien moeten worden of dit de mogelijkheden voor nu geaccepteerde vormen van verder verwerken niet belemmert.

Beslispunt

Beleidslijn
d. De Belastingdienst zet in op handhaving van de bestaande invulling van het beginsel van doelbinding en verder verwerken, zodat gegevens optimaal kunnen worden ingezet voor de uit te voeren taken. Daarbij worden waar nodig beschermende maatregelen getroffen, waarbij kan worden gedifferentieerd naar gebruik en gebruikers van de gegevens.

Naar aanleiding van bespreking van deze beleidslijn in het DT van 24 mei 2018 heeft met Toeslagen en KI&S nog overleg plaatsgevonden over een aantal casusposities. Daaruit is naar voren gekomen dat de beleidslijn onveranderd blijft. Compliance is ook bij dienstverlening de basis voor het handelen en dat onderstreept onze invulling van het beginsel van doelbinding (dus inclusief dienstverlening). Van belang blijft om vanuit imago perspectief zelfs de schijn van niet voldoen aan de AVG op dit punt, dat wil zeggen een te ruime interpretatie van doelbinding en daardoor een gegevensverwerking zonder afdoende grondslag, te vermijden. Daaruit volgt een actie en een advies (dat inmiddels deels is overgenomen):

Actie Toeslagen
De uitwisseling van gegevens met o.a. DUO en UWV ten behoeve van actieve signalering van burgers om hoge terugvordering te voorkomen wordt in overleg met DGFZ nader beoordeeld op toereikendheid van de wettelijke grondslag.

[1] De verwerking van persoonsgegevens voor opsporingsdoeleinden wordt niet gereguleerd door de AVG, maar door de Richtlijn gegevensverwerking opsporing en vervolging. Ook deze kent echter de eis van doelbinding.

Advies aan KI&S
Het door de burger vermelde telefoonnummer in de aangifte IB wordt voor meerdere doeleinden gebruikt. De toelichting in het aangifteformulier geeft aan dat dit nummer alleen wordt gebruikt voor vragen over de betreffende aangifte. Voor verder/breder gebruik van het telefoonnummer moet uitdrukkelijk(er) toestemming aan de burger worden gevraagd. De toelichting op MBD/OLAV is met het oog hierop sinds de aangiftecampagne 2017 ruimer geformuleerd (... kunnen we u bereiken... *bijvoorbeeld* naar aanleiding van uw aangifte...).
Met betrekking tot toestemming als verwerkingsgrond zijn nog geen mogelijkheden ingeregeld zoals het gestructureerd vastleggen van de toestemming en het kunnen intrekken, anders dan vragen om correctie en om wissen van gegevens. Aangezien er behoefte is aan dit gegeven in verband met communicatiemogelijkheden (bv. inzet van sms), is het wenselijk om voorzieningen te creëren (bijvoorbeeld CRM gekoppeld aan interactie via portalen) waarin het voor de burger makkelijk is om o.a. zijn contactgegevens te kunnen aanpassen en toestemming voor gebruik ook weer in te trekken.

3.1.3 Informatieplicht en transparantie
Artikel 12 regelt de wijze waarop voldaan moet worden aan de informatieplicht, die nader uitgewerkt is in artikel 13 en 14. Artikel 12 regelt het 'hoe', artikel 13 en 14 het 'wat'. Ze geven uitwerking aan het beginsel van *transparantie*. Artikel 12 schrijft voor dat de verwerkingsverantwoordelijke passende maatregelen neemt om informatie over verwerkte persoonsgegevens te verstrekken in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm. De artikelen 13 en 14 geven een opsomming van de te verstrekken informatie (strikt genomen zijn dit gesloten normen, maar vanwege de samenhang met artikel 12 worden ze hier besproken).

De Belastingdienst vervult deze verplichting door middel van een privacypagina op de website waarop ook een overzicht van gegevensverwerkingen wordt opgenomen. Het AVG-register wordt vooralsnog niet integraal gepubliceerd; het register is primair bestemd voor toezicht en publicatie is niet verplicht. In dit stadium leent het register zich nog niet voor communicatieve doeleinden; dat vraagt nog een kwaliteitsslag in de beheerfase. Het DT heeft op 26 april met deze lijn ingestemd. Inmiddels heeft hierover ook overleg plaatsgevonden met de FG, die met de wijze van vervullen van de informatieplicht en het niet publiceren van het AVG-register heeft ingestemd, maar wel aandacht vraagt voor het doorvoeren van de benodigde kwaliteitsslag.

Artikel 14, vijfde lid, geeft een uitzondering op de informatieplicht, namelijk als het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven in wetgeving en die wetgeving passende maatregelen bevat om de gerechtvaardigde belangen van betrokkenen te beschermen. In het algemeen wordt aangenomen dat indien de verkrijging van de gegevens gebaseerd is op algemeen verbindende voorschriften die bekendgemaakt zijn, daarmee aan de informatieplicht wordt voldaan. Hoewel deze uitzondering op de Belastingdienst van toepassing is, omdat de verkrijging van gegevens door de Belastingdienst op basis van wetgeving geschiedt, is het wenselijk om informatie over van derden verkregen gegevens wel op te nemen in het overzicht van verwerkingen en dus geen gebruik te maken van deze uitzonderingsgrond. Maximale transparantie kan bijdragen aan het vertrouwen in de Belastingdienst.

Beslispunt

Beleidslijnen
e. De Belastingdienst vervult de informatieplicht door middel van een privacypagina op de website waarop ook een overzicht van

gegevensverwerkingen wordt opgenomen. Het AVG-register wordt vooralsnog niet integraal gepubliceerd (DT-besluit van 26 april 2018).
f. De Belastingdienst maakt met het oog op maximale transparantie naar betrokkenen, geen gebruik van de uitzondering op de informatieplicht.

Actie
g. In het kader van het beheer van het AVG-register (belegd bij IV&D) worden verdere kwaliteitsverbeteringen doorgevoerd zodat het register per 1 april 2019 integraal gepubliceerd kan worden.

3.1.4 Geautomatiseerde besluitvorming
In artikel 22 AVG is bepaald dat een betrokkene het recht heeft niet onderworpen te worden aan een op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan rechtsgevolgen zijn verbonden of dat hem in aanmerkelijk mate treft.
In artikel 40 van de Uitvoeringswet AVG wordt geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, toegestaan indien dat noodzakelijk is voor de vervulling van een taak van algemeen belang. De Belastingdienst maakt in ruime mate gebruik van geautomatiseerde besluitvorming (bv. opleggen belastingaanslagen, toekennen en continueren van toeslagen). Op grond van artikel 40 van de Uitvoeringswet AVG is dit toegestaan.

Profilering wordt in de AVG (artikel 4) gedefinieerd als "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen."
Waar in de uitvoeringspraktijk van de Belastingdienst gesproken wordt over profielen, zijn dit geen profielen volgens de definitie van de AVG. Profielen worden gebruikt om posten/dossiers risicogericht te selecteren, en die handmatig te behandelen. Bijvoorbeeld het anders behandelen van een eerste toeslagaanvraag vanwege een verhoogd risico. Of het afwijkend behandelen van aangiften vallend onder een HT convenant, vanwege de risicoreductie die het convenant met zich meebrengt. Uitworp voor toezicht op basis van een risicoprofiel leidt dus juist tot beoordeling door een mens. Ook in die gevallen waarin zonder handmatige tussenkomst correcties worden opgelegd (de zogenaamde stellige correcties) is geen sprake van profilering in de zin van de AVG, maar is sprake van een onder de AVG toegestaan geautomatiseerd besluit op basis van objectieve kenmerken door vergelijking van beschikbare gegevens. Bovendien is op deze besluiten de normale rechtsbescherming van bezwaar en beroep van toepassing.

Op grond van de AVG en de Uitvoeringswet AVG kan de huidige praktijk van geautomatiseerde besluitvorming bij de Belastingdienst worden voortgezet, maar specifieke actie is nog nodig om 'nuttige informatie' te geven aan betrokkenen over de logica die aan geautomatiseerde besluiten ten grondslag ligt.
Op dit moment geeft de Belastingdienst op de website informatie over de processen waarin geautomatiseerde besluitvorming wordt ingezet en de wijze waarop dit gebeurt. Verder ligt informatie omtrent de logica opgesloten in de wijze waarop de Belastingdienst de (elektronische) hulpmiddelen vormgeeft (bijvoorbeeld formulieren, online aangiftevoorziening). Dit laatste is nog nadrukkelijker beschreven in de privacyverklaring en informatie hierover zal nog worden opgenomen in het verwerkingenregister. Daarmee geeft de

Belastingdienst naar de huidige inzichten voldoende uitvoering aan de eisen in de AVG.
Daarnaast neemt de Belastingdienst deel in de interdepartementale werkgroepen die het kabinetsstandpunt bij het WRR-rapport over Big Data vertalen naar rijksbrede richtsnoeren voor transparantie en inzicht in algoritmen. Op basis van die richtsnoeren past de Belastingdienst de hierboven beschreven praktijk waar nodig aan.

Beslispunt

Beleidslijn
h. De Belastingdienst houdt subjectgericht toezicht, gebaseerd op risicoselectie aan de hand van objectieve kenmerken. Profielen op basis van dergelijke kenmerken worden ingezet voor selectie van dossiers voor toezicht of klantbehandeling. Dergelijke profielen zijn geen product van profilering in de zin van de AVG. Onze huidige uitvoeringspraktijk valt daarmee binnen de grenzen die de AVG daaraan stelt.

3.1.5 Beperkingsmogelijkheid rechten van betrokkenen
Artikel 23 jo. artikel 41 Uitvoeringswet AVG, biedt de mogelijkheid om de rechten van betrokkene en de vervulling van verplichtingen door de verwerkingsverantwoordelijke te beperken in het licht van (oa.) belangrijke financiële en economische belangen (waaronder fiscale aangelegenheden en sociale zekerheid), en voor taken van inspectie en toezicht op genoemde terreinen. De bevoegdheid tot beperking ligt bij de verwerkingsverantwoordelijke Deze bepalingen raken de beginselen van *rechtmatigheid, behoorlijkheid en transparantie*.

Het gaat hier om het beperken van informatieplicht (zie 3.1.3) en onder meer het recht op inzage (zie 3.2.5) in specifieke gevallen. Gedacht kan worden aan strategische handhavingsbelangen die het geven van inzage in bepaalde gegevens onwenselijk maken. Er zullen concernbrede criteria ontwikkeld moeten worden voor het beoordelen of daarvan in bepaalde gevallen sprake is. In het licht van kenbaarheid en transparantie ligt het in de rede deze kaders in beleidsregels vast te leggen.

Beslispunt

Actie
i. De Concerndirectie UHB ontwikkelt (in samenspraak met FJZ en IV&D) kaders voor het beperken van rechten van betrokkenen onder de AVG.

3.1.6 Privacy by design en by default
Artikel 25 AVG regelt de verplichting om bij de bepalen van de verwerkingsmiddelen en bij de verwerking zelf passende technische en organisatorische maatregelen te nemen die de beginselen uit de AVG op een doeltreffende manier uitvoeren en om daarin de nodige waarborgen in te bouwen ter naleving van de AVG (*privacy by design*). Daarnaast moeten maatregelen worden getroffen die ervoor zorgen dat in principe alleen de gegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking (*privacy by default*). Deze principes omvatten eigenlijk alle eerdergenoemde beginselen.

Privacy by design en privacy by default impliceren dat in alle stadia van ontwikkeling, van wetgevingsvoorbereiding tot feitelijk ontwerp van systemen en processen, rekening wordt gehouden met het aspect privacy. Het begint dus in feite al in het traject van ontwikkeling van beleid en wetgeving: hoe wordt het beleid geïnstrumenteerd, is het nodig om daarbij persoonsgegevens te

verwerken en zo ja, welke? Staat de verwerking in verhouding tot het beoogde doel? De toets op privacy aspecten in dit vroege stadium gebeurt door DGFZ, in samenspraak met UHB, FJZ en IV&D. Vervolgens worden de privacyaspecten bij uitvoeringstoetsen in kaart gebracht, als meer zicht bestaat op de concrete vormgeving van de gegevensverwerking. Het privacyaspect en de rol van de pIA daarin is inmiddels verwerkt in de documentatie en werkwijze van de UTNS.

Het toetsen van privacyaspecten in dit vroege stadium van ontwerp is noodzakelijk, maar kent inherent beperkingen door de mate van concreetheid van de te toetsen producten. Voortschrijdende inzichten kunnen alsnog privacyproblemen aan het licht brengen. Deze problemen zijn ofwel in het ontwerp te ondervangen door middel van mitigerende maatregelen ofwel leiden tot fundamentele tekortkomingen in het naleven van de privacybeginselen. In dergelijke gevallen is consultatie van de AP noodzakelijk (zie ook 3.2.9.). Gevolg hiervan kan zijn dat initiële oordeel omtrent uitvoerbaarheid moet worden bijgesteld.

De wijze waarop de Belastingdienst invulling geeft aan de genoemde principes is het verankeren ervan in architectuurprincipes en het toepassen van MTHV's (methoden, technieken, hulpmiddelen en voorschriften) in het ontwerptraject van processen en IV-voorzieningen.

Beslispunten

Beleidslijnen
j. Privacy by design en by default betekent onder andere het al bij wetsvoorbereiding leveren van input op PIA's, en het uitvoeren van een PIA door de Belastingdienst zelf, zodra er concreter zicht is op de inhoud van de gegevensverwerking (zie ook paragraaf 3.1.10).
k. Privacy by design en by default betekent ook het expliciet betrekken van privacyaspecten bij het uitvoeren van een UTNS op concept-wetgeving.

Acties
l. UHB maakt, in afstemming met IV&D, afspraken met DGFZ over betrokkenheid bij het uitvoeren van PIA's in de fase van voorbereiding van wetgeving.
m. Ontwerpproducten worden door IV&D getoetst aan de architectuurkaders, waarin privacy by design en by default zijn verankerd.
n. Onder regie van IV&D worden privacy by design en by default uitgewerkt in concrete voorschriften voor ontwerp van processen en van IV-voorzieningen. IV houdt toezicht op de toepassing daarvan (first line of defense).

3.1.7 Verwerkers
Artikel 28 bepaalt dat de verwerkingsverantwoordelijke alleen een beroep doet op verwerkers die afdoende garanties bieden dat de verwerking voldoet aan de vereisen van de AVG en de bescherming van betrokkenen is gewaarborgd. Hiermee wordt invulling gegeven aan beginselen van *rechtmatigheid*, *integriteit* en *vertrouwelijkheid*.

Een belangrijk instrument hierbij is de verwerkersovereenkomst, waarin de verwerking door de verwerker wordt geregeld. Bij de inventarisatie van verwerkingen in het AVG-register is in kaart gebracht voor welke verwerkingen een verwerker wordt ingezet, en of een overeenkomst is gesloten. Voor enkele tientallen verwerkingen is onzeker of er een overeenkomst aanwezig is en/of nog een overeenkomst gesloten moet worden. De onderdelen zorgen ervoor dat waar voor hun verwerkingen nog overeenkomsten ontbreken, deze uiterlijk eind 2018 zijn afgesloten.

Het sluiten van overeenkomsten is één ding, maar er moet ook verzekerd zijn dat de daarin gemaakte afspraken worden nagekomen. In de model-verwerkersovereenkomsten bij de Arvodi en Arbit (de algemene rijksvoorwaarden voor het verrichten van (ICT-)diensten) is een bepaling opgenomen over verantwoording van de verwerker over het naleven van de AVG, door informatieverstrekking en via periodieke onafhankelijke audits door de opdrachtgever of door de verwerker zelf. De Belastingdienst maakt gebruik van deze modelovereenkomsten.

Beslispunten

Beleidslijnen
o. Leveranciers die als verwerker optreden voor de Belastingdienst, verantwoorden zich over de naleving van verwerkersovereenkomsten via de daarvoor in die overeenkomsten opgenomen afspraken.
p. Voor verwerkersovereenkomsten wordt gebruik gemaakt van de modelovereenkomsten bij Arvodi en Arbit.

Acties
q. De dienstonderdelen sluiten voor eind 2018 verwerkersovereenkomsten af voor gegevensverwerkingen waarvoor deze nog ontbreken.

3.1.8 Informatiebeveiliging

Artikel 32 AVG bepaalt dat, rekening houdend met de technische mogelijkheden, passende technische en organisatorische maatregelen getroffen moeten worden om een op de aan de verwerking verbonden risico's afgestemd beveiligingsniveau te realiseren. Als concrete maatregelen worden onder meer (waar passend) pseudonimisering en versleuteling genoemd. Dit is invulling van de beginselen van *integriteit*, *vertrouwelijkheid* en *minimale gegevensverwerking*.

Het beveiligingsbeleid is neergelegd in het Handboek Beveiliging Belastingdienst (HBB). Het HBB mist echter op een aantal gebieden nog de concreetheid die in de operatie nodig is. Voorbeelden van onderwerpen waarvoor dit geldt (blijkend uit praktijkvragen die aan het programma AVG zijn voorgelegd) en mogelijk daarbij te volgen beleidslijnen zijn:

- Informatiebeveiliging omvat autorisatie, als vorm van toegangsbeveiliging en uitwerking van het principe van *need to know*. Het is niet altijd duidelijk waar de grens van need to know ligt.
  De bestaande wijze van autoriseren, gebaseerd op taken en functies, is een algemeen geaccepteerde handelwijze. Aan het toekennen van autorisaties door de direct leidinggevende ligt de filosofie ten grondslag dat medewerkers de autorisaties krijgen waarmee ze hun werk naar behoren kunnen uitvoeren. Uitgangspunten daarbij zijn integrale klantbehandeling (hetgeen leidt tot brede autorisatie voor verschillende belastingmiddelen) en landelijke inzet. Deze uitgangspunten worden binnen de huidige mogelijkheden van de techniek en binnen de algemene geheimhoudingsplicht en de continue aandacht voor bewustwording bij het omgaan met gegevens, acceptabel geacht.
  De voortschrijdende techniek maakt meer gedifferentieerde autorisatie mogelijk, die beter tegemoet komt aan de beginselen van vertrouwelijkheid en integriteit, maar ook van doelbinding (zie ook 3.1.2). Dit kan worden gebaseerd op dynamische toekenning van autorisaties bij de uitgifte van werk. Deze nieuwe technische mogelijkheden dienen, onder regie van IV&D in samenwerking met sso F&MI, nader worden uitgewerkt in beleids- en ontwerpprincipes.

Naast de ontwikkeling van nieuwe technische mogelijkheden is continu aandacht nodig voor de actualiteit van de bestaande autorisaties. Dit reguliere beheerproces vraagt expliciete aandacht van de lijnorganisatie, waarbij sso F&MI ondersteuning biedt.

De bestaande praktijk van interne verstrekking van gegevens is onvoldoende gebaseerd op de principes van integriteit, vertrouwelijkheid en minimale gegevensverwerking. Persoonsgegevens, worden breed in de organisatie beschikbaar gesteld, waarbij niet of onvoldoende rekening wordt gehouden met het need to know-principe. Het is van belang om de noodzaak tot gegevensverstrekking expliciet te valideren aan de hand van minimaal een WMK toets. Met de belangrijkste interne gegevensverstrekkers is deze afspraak gemaakt.
In het verlengde hiervan moeten faciliteiten voor datadumping (applicatieve voorziening om data buiten de reguliere applicatie te kunnen ontsluiten) en uitwisselgebieden (voorzieningen zoals Wisselland) worden uitgefaseerd dan wel worden voorzien van sluitende autorisatiemechanismen. Tenslotte wordt beperking van de interne verstrekking van gegevens versterkt door een heldere afbakening van verantwoordelijkheden tussen CAP, F&MI, DF&A en IV.

- Pseudonimiseren is wat betreft werkbaarheid en de technische mogelijkheden nog niet breed inzetbaar bij de Belastingdienst. De ervaringen die nu bij DF&A worden opgedaan, worden betrokken bij de keuze waar en hoe deze maatregel wordt ingezet.

- Productiedata worden op grote schaal gebruikt voor testdoeleinden. Daardoor worden de gegevens buiten de formele, in de systemen opgenomen, autorisatiestructuur breder toegankelijk dan noodzakelijk. Dit is in strijd met het need to know principe.
  Het testen van systemen dient dan ook te geschieden met fictieve testdata dan wel met gepseudonimiseerde productiegegevens. De Belastingdienst sluit aan bij rijksbrede initiatieven voor het ontwikkelen van generieke sets met testdata (het zogenoemde 'testdorp').

  In gevallen waarin testen met productiedata onvermijdelijk is, moet dit met strenge waarborgen zijn omkleed. Deze waarborgen worden door IV&D in samenwerking met CAP en IV geformuleerd. Een van de zaken die daarbij – vanuit oogpunt van beheersing van gebruik van productiegegevens voor testdoelen – meegenomen moet worden, is het beleggen van het eigenaarschap van de test/acceptatieomgeving en van daarin in bijzondere gevallen te gebruiken productiedata.

- Als gegevens buiten de Belastingdienst worden gebracht, gebeurt dat altijd in versleutelde vorm.

- Toegang tot en gebruik van personeelsgegevens, als verbijzonderde vorm van persoonsgegevens, moet voldoen aan de beginselen van de AVG. Toegang en gebruik van personeelsgegevens via de formele systemen is omgeven door de standaard toegangs- en beveiligingsmaatregelen die, met inachtneming van de afgesproken beleidslijnen, voldoen aan de (AVG) eisen.
  Personeelsgegevens worden echter ook buiten de formele systemen om ter beschikking gesteld, ter ondersteuning van onder meer lokale personeelsprocessen en operationele sturing. Deze praktijk van interne verstrekking van personeelsgegevens is onvoldoende gebaseerd op de

principes van integriteit, vertrouwelijkheid en minimale gegevensverwerking en de lokale applicaties kennen over het algemeen geen relatie met de autorisatiestructuur in de formele systemen (IMS).

Personeelsdossier
Voor beheer van het personeelsdossier maken we gebruik van P-Direkt. In P-Direkt is toegang tot het personeelsdossier geregeld door middel van het rollenmodel. Het rollenmodel is de vertaling van de organisatorische verantwoordelijkheidsverdeling. Nevengeschikte managers hebben geen recht op toegang tot de personeelsgegevens van medewerkers van hun collega's, tenzij er sprake is van een formele vervanging. Bovengeschikte managers hebben recht op toegang tot de personeelsgegevens van alle direct en indirect onder hen ressorterende medewerkers. Het rollenmodel strookt ook met de AVG: toegang tot persoonsgegevens van medewerkers is voor bovengeschikte leidinggevenden noodzakelijk in het licht van een gerechtvaardigd belang, namelijk het kunnen aansturen van personeel en voeren van personeelsbeleid.
Het gebruik van P-Direkt past bij het aansluiten op rijksstandaarden en levert in de praktijk geen evidente problemen op. Op 24-5- is besloten (actie 22 uit het gecompileerde overzicht) dat de concerndirectie O&P voor eind 2018 een heroriëntatie uitvoert op het applicatie landschap voor bedrijfsvoering, gericht op een dominantere plaats van P-Direkt daarbinnen. Het benutten van meer functionaliteiten van P-Direkt maakt het mogelijk het applicatielandschap structureel te vereenvoudigen, waardoor ook het gebruik van personeelsgegevens beter wordt beheerst.

Operationele sturing
Voor de besturing van teams biedt P-Direkt biedt geen functionaliteit. Er is een combinatie van meta informatie uit het primair proces en personeelsgegevens nodig om vast te stellen welke capaciteit noodzakelijk is, wie op welk dossier ingezet kan worden, hoe de leidinggevende zich kan verantwoorden naar zijn/haar leidinggevende etc..

Applicaties die wel tegemoet komen aan bovenstaande behoeften zijn nu over het algemeen lokaal ontwikkeld en worden gevoed door interne verstrekking van personeelsgegevens. Deze praktijk is onvoldoende gebaseerd op de principes van integriteit, vertrouwelijkheid en minimale gegevensverwerking en de applicaties kennen over het algemeen relatie met de autorisatiestructuur zoals we die in de formele systemen kennen (IMS). Uitgangspunt is dat deling van personeelsgegevens niet is toegestaan, tenzij de noodzaak daartoe is vastgesteld. Sanering van deze applicaties is gelet daarop wenselijk en daarnaast moeten hiervoor vervangende voorzieningen worden ontwikkeld.

Specifieke personeelsgegevens
Specifieke personeelsgegevens betreffen gegevensverzamelingen die behoren bij bedrijfsmiddelen van de Belastingdienst en het vastleggen van gegevens daaruit. Het gaat bijvoorbeeld om bestanden die behoren bij (draagbare) computers, printers, (draagbare) telefoons, toegangsbeveiligingsapparatuur, trafficcontrolapparatuur en bewakingscamera's en soortgelijke bedrijfsmiddelen. Toegang tot dergelijke bestanden wordt zeer beperkt verleend. Het op de organisatorische verantwoordelijkheidsverdeling

gebaseerde rollenmodel van P-Direkt is hiervoor te ruim. In de Personele Uitvoeringsbepalingen Belastingdienst (PUB) / Integriteit (hoofdstuk 7 paragraaf 4.5) wordt geregeld dat, in het geval van een onderzoek naar vermoedelijk plichtsverzuim door een medewerker van de Belastingdienst, toegang tot dergelijke gegevensverzamelingen alleen mogelijk is na voorafgaande toestemming. Aan deze uitvoeringsbepalingen wordt onverkort vastgehouden.

Beslispunten

Beleidslijnen

r. Autorisatiebeleid is gebaseerd op principes als integrale klantbehandeling en landelijke inzet van medewerkers. Daarbij wordt – met gebruikmaking van beschikbare technieken – gedifferentieerd naar de aard van het gebruik van de gegevens (het werk waarvoor ze worden ingezet) en de aard van de gegevens zelf.

s. Voor elke interne verstrekking van gegevens wordt een WMK-toets uitgevoerd.

t. Faciliteiten voor datadumping (applicatieve voorziening om data buiten de reguliere applicatie te kunnen ontsluiten) en voorzieningen voor grootschalig hergebruik zoals Wisselland worden uitgefaseerd, tenzij de noodzaak voor gebruik kan worden onderbouwd. In dat geval worden zij voorzien van sluitende autorisatiemechanismen.

u. Er worden geen productiedata gebruikt voor testdoeleinden; testen geschiedt met fictieve testdata dan wel met gepseudonimiseerde productiedata. Aangesloten wordt bij rijksbrede initiatieven zoals het 'testdorp'. Als testen zonder (gepseudonimiseerde) productiedata onvermijdelijk is, wordt extra maatregelen getroffen om de bescherming van de gegevens te waarborgen.

ua. Toegang tot en gebruik van personeelsgegevens, als verbijzonderde vorm van persoonsgegevens, moet voldoen aan de eisen van de AVG. Het gerechtvaardigd belang van de werkgever brengt met zich mee dat de toegang tot gegevens wordt verleend conform de organisatorische verantwoordelijkheids-verdeling. Dit geldt zowel voor toegang tot personeelsdossiers als voor het ter beschikking stellen van informatie ten behoeve van het operationeel sturen en verantwoorden. Voor toegang tot specifieke personeelsgegevens, gekoppeld aan het gebruik van bedrijfsmiddelen van de Belastingdienst en het vastleggen van gegevens daaruit, blijven de specifieke afspraken uit het PUB onverkort van toepassing.

Acties

v. Elk dienstonderdeel toetst voor 1 oktober 2018 actief de actualiteit van bestaande autorisaties en neemt maatregelen om niet actuele autorisaties in te trekken. Dit wordt ondersteund en gemonitord door sso F&MI; eind oktober brengt F&MI hierover een rapportage uit aan het DT.

w. De concerndirectie IV&D werkt in overleg met sso F&MI nieuwe technische mogelijkheden op het gebied van autoriseren uit in beleids- en ontwerpprincipes

x. De concerndirectie O&P brengt voor 25 mei 2018 met de grootste verwerkers van personeelsgegevens in beeld welke personeelsgegevens worden gewisseld, alsmede de noodzaak voor die gegevensverwerkingen; waar issues geconstateerd worden ten aanzien van de noodzaak, worden applicaties uitgefaseerd. Indien dat onoverkomelijke problemen geeft voor de continuïteit, worden maatregelen geformuleerd.

xa. Met het oog op vervanging van bestaande LOA's wordt nader onderzoek gedaan naar ontwikkeling van datafundamenten voor personeelsgegevens met bijbehorende dashboards, ten behoeve van operationeel sturen en verantwoorden.

y. De concerndirectie O&P voert voor eind 2018 een heroriëntatie uit op het applicatieve landschap voor bedrijfsvoering, gericht op een dominantere plaats van P-Direkt daarbinnen waar het personeelsgegevens betreft.
z. De ketendirecteur gegevens neemt het initiatief om voor 1 oktober 2018 te komen tot afspraken over heldere afbakening van verantwoordelijkheden tussen CAP, F&MI, DF&A en IV.
aa. De concerndirectie IV&D werkt in samenwerking met IV en CAP kaders uit voor de waarborgen bij testen met productiedata. Daarbij wordt expliciet aandacht besteed aan het eigenaarschap van de test/acceptatieomgevingen de verantwoordelijkheid voor daarin gebruikte productiegegevens.

3.1.9 Informatieplicht bij datalekken
Op grond van artikel 34 AVG moet de verwerkingsverantwoordelijke de betrokkenen informeren over een datalek, in geval die waarschijnlijk een hoog risico inhoudt voor hun rechten en vrijheden. Dit geeft invulling aan de beginselen van *behoorlijkheid* en *transparantie*.

Deze verplichting hangt samen met de meldplicht datalekken van artikel 33. Criteria voor het bepalen wanneer sprake is van een dermate hoog risico dat het informeren van betrokkenen aan de orde is, zijn opgenomen in de procedure voor melding van datalekken (zie 3.2.7).

Geen beslispunt

3.1.10 Privacy Impact Assessment
Op grond van artikel 35 is de verwerkingsverantwoordelijke verplicht om voor gegevensverwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen een PIA uitvoeren. Met het uitvoeren van een PIA worden risico's ten aanzien van alle beginselen in kaart gebracht en maatregelen getroffen die naleving van de beginselen verzekeren.
Voor het uitvoeren van PIA's en de gevallen waarin dat moet gebeuren is een handleiding opgesteld. Daarin zijn ook de verantwoordelijkheden, bevoegdheden en taken van betrokkenen bij het PIA-proces binnen de Belastingdienst beschreven. Het concept is in het DT van 26 april jl. geaccordeerd en zal nog worden afgestemd met de FG en de medezeggenschap.
In dat DT is tevens afgesproken dat voor eind 2018 de PIA's die nog uitgevoerd moeten worden op bestaande verwerkingen (op grond van signalering in het AVG-register) worden afgerond.

Beslispunt

Acties
bb. Het programma AVG zorgt voor afstemming van de concept-handleiding PIA met FG en medezeggenschap en voor voorlegging aan het DT ter vaststelling (besluit DT van 26 april 2018).
cc. De dienstonderdelen zorgen voor het uiterlijk eind 2018 afronden van nog uit te voeren PIA's (besluit DT van 26 april 2018).

3.1.11 Doorgifte van persoonsgegevens naar derde landen
De artikelen 44 tot en met 46 geven een aantal verplichtingen waaraan moet worden voldaan bij doorgifte van persoonsgegevens naar derde landen. Dit dient de *rechtmatigheid* en *behoorlijkheid*.

Nederland heeft zich op grond van verschillende Europese en internationale regelingen en afspraken verplicht tot automatische uitwisseling van gegevens, waarbij elk land op basis van de vertrouwelijkheids- en gegevensbeschermingstoetsen van een ander land kan beslissen of dat land

voldoet aan de eisen die het stelt aan de vertrouwelijkheid en gegevensbescherming. In de UTNS AVG is aangegeven dat in feite voor alle landen waaraan gegevens worden geleverd (zowel op grond van verplichtingen vanuit de OESO, vanuit de Europese Commissie als op grond van MOU's) moeten worden getoetst of zij voldoen aan de criteria die de AVG stelt. Daarbij is voor Europese regelingen voorgesteld wordt om nu nog geen actie te ondernemen, maar af te wachten of de Commissie zelf met een plan komt voor toetsing van die regelingen aan de AVG. Voor de bilaterale verdragen zou een nadere doorlichting nodig zijn om de gevolgen van de AVG goed in kaart te brengen en de nodige maatregelen (bv. wijziging) te kunnen treffen. Deze heeft onder de basispositie nog niet plaatsgevonden, maar zou voor eind van het jaar wel ter hand genomen moeten worden om risico's en issues in kaart te krijgen en maatregelen te formuleren, zodat de Belastingdienst ook hierop in control komt.

Beslispunten

Beleidslijn
dd. De Belastingdienst onderneemt niet zelfstandig actie op toetsing van EU-regelingen voor informatie-uitwisseling met derde landen aan de vereisten van de AVG.

Actie
ee. De dienstonderdelen toetsen voor eind 2018 hun bilaterale verdragen met landen buiten de EU op het bieden van een vergelijkbaar beschermingsniveau met de AVG. Als dat niet het geval is, of als daarover twijfel bestaat, wordt de verstrekking stopgezet.

3.2 Gesloten normen

3.2.1 Rechtmatigheid
Artikel 6, eerste en derde lid, werkt het beginsel van *rechtmatigheid* uit. Gegevensverwerking is alleen rechtmatig indien deze berust op toestemming, noodzakelijk is ter uitvoering van een overeenkomst, ter bescherming van vitale belangen van de betrokkene, naleving van een wettelijke plicht, uitvoering van een taak van algemeen belang die in wetgeving is vastgelegd, of ter behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke of de wederpartij.

Gegevensverwerking voor de primaire processen van de Belastingdienst geschiedt op basis van taken van algemeen belang die zijn vastgelegd in (met name) de Awr, Awir, Invorderingswet en Algemene douanewet. Verstrekking van gegevens aan andere overheidsorganisaties (zoals UWV, SVB en gemeenten ten behoeve van toezicht op socialezekerheidswetgeving) geschiedt op basis van een wettelijke plicht. Daarnaast worden gegevens verstrekt op grond van doorbreking van de geheimhoudingsplicht (artikel 67 Awr jo. 43c Uitvoeringsregeling Awr of een ontheffing van de Minister van Financiën), aan overheidsorganisaties die deze mogen verwerken op grond van hun wettelijk vastgelegde taak van algemeen belang. In dat geval wordt beoordeeld of sprake is van een verenigbaar doel voor de ontvangende organisatie (zie 3.1.1).

Gegevensverwerking voor secundaire processen (bedrijfsvoering) geschiedt op grond van (noodzaak ter behartiging van) een gerechtvaardigd belang. De grens tussen noodzaak en wenselijkheid is vaak diffuus. Hiervoor zouden (net als bij het eerder genoemde *need to know*-principe in het kader van informatiebeveiliging) criteria ontwikkeld moeten worden.

Toestemming wordt door de Belastingdienst in beginsel niet gebruikt als grondslag voor het verwerken van gegevens, vanwege de afhankelijke positie tussen burgers en de dienst. Burgers hebben geen alternatief voor veel zaken die zij met de Belastingdienst kunnen of moeten doen, zodat toestemming niet echt vrijwillig verleend zou worden. Hetzelfde geldt voor verwerking van personeelsgegevens; ook hier is toestemming niet geschikt vanwege de afhankelijkheidsrelatie tussen werknemer en werkgever.
In dit licht is de gegevensverwerking door Shuttel, de leverancier van de mobiliteitskaart problematisch. Deze vindt plaats op grond van levering door BZK van gegevens uit P-direkt aan de leverancier, op grond van impliciete toestemming van betrokkenen, waaronder medewerkers van MinFin en de Belastingdienst. De Minister van BZK is verwerkingsverantwoordelijke voor deze gegevens, en als zodanig ook aansprakelijk voor eventuele gebreken in de verwerking daarvan door verwerkers zoals Shuttel. Uitgangspunt is dat deze verantwoordelijkheid bij BZK wordt gelaten; de Belastingdienst neemt het initiatief om dit gebrek bij BZK onder de aandacht te brengen en aan te dringen op maatregelen om dit weg te nemen.

Toestemming kan bijvoorbeeld wel worden ingezet voor enquêtes/onderzoeken ten behoeve van verbetering van de dienstverlening e.d. (waarbij dan geen tegenprestaties aan het deelnemen verbonden moeten worden (dit gebeurt soms wel)).

Bij de inventarisatie van gegevensverwerkingen is naar voren gekomen dat er een aantal verwerkingen is waarvan de grondslag onbekend of niet duidelijk is. Het betreft met name inwinstromen bij CAP. Een nadere analyse van deze stromen is nodig om te bepalen of de grondslag afdoende is. Zo niet, dan zal moeten worden bezien wat de risico's zijn bij voortzetting van het inwinnen, en zal met DGFZ overlegd moeten worden over het creëren van een grondslag. Dat gesprek kan plaatsvinden in het kader van de wetgeving voor gegevensverwerking door de Belastingdienst die DGFZ in voorbereiding heeft. Deze zal overigens niet voor 2020 in werking treden. Voor bijvoorbeeld het inwinnen en verwerken van het BSN in het kader van IB47 is al eerder vastgesteld dat de grondslag ondeugdelijk is. Daarvoor wordt gezocht naar een tussentijdse oplossing.

Beslispunten

Beleidslijnen
ff. De verantwoordelijkheid voor rechtmatige verwerking van personeelsgegevens in het kader van de mobiliteitskaart ligt bij BZK.
gg. Toestemming als grondslag voor verwerking van persoonsgegevens wordt alleen toegepast voor enquetes/onderzoeken ter verbetering van dienstverlening. Er wordt geen tegenprestatie verbonden aan deelname.

Acties
hh. Sso CFD en CD O&P nemen het initiatief om bij BZK aan te dringen op herstel van het gebrek in de grondslag voor gebruik van gegevens voor de Shuttelkaart.
jj. CAP levert bij de concerndirectie IV&D een overzicht aan van inwinstromen waarvan de grondslag niet duidelijk is. Op basis van analyse van de opgevoerde verwerkingen voeren IV&D en FJZ overleg met DGFZ over het waar nodig creëren van een adequate grondslag. Dit overleg omvat tevens het creëren van een (tussen)oplossing voor BSN-verwerking in het kader van het IB47-proces.

3.2.2 Voorwaarden bij toestemming als grondslag voor verwerking

De artikel 7 en 8 stellen een aantal voorwaarden indien toestemming als grondslag voor de verwerking wordt gebruikt, als invulling van het beginsel van *rechtmatigheid* en *behoorlijkheid.*

Dit betreft bijvoorbeeld het kunnen aantonen dat de betrokkene toestemming heeft gegeven en vormvoorschriften voor het verzoek om toestemming en het specifieke regels voor toestemming indien het gaat om kinderen onder 16 jaar. In het kader voor gebruik van toestemming zouden de wijze van vastleggen en aantonen van de toestemming moeten worden opgenomen.

Beslispunt

Actie
kk. In het kader voor gebruik van toestemming als grondslag voor gegevensverwerking (zie 3.2.1) worden de voorwaarden bij toepassing van toestemming vastgelegd.

3.2.3 Bijzondere persoonsgegevens
Artikel 9 regelt de verwerking van bijzondere persoonsgegevens, zoals gegevens over ras of etnische afkomst, geaardheid, geloof, lidmaatschap van een vakbond en gezondheid. Ook dit betreft uitwerking van het beginsel van *rechtmatigheid.*
De AVG gaat uit van een verbod op het verwerken van deze gegevens maar biedt de mogelijkheid om hierover een regeling te treffen in het nationale recht. Dat is gebeurd in de Uitvoeringswet AVG.

De Belastingdienst verwerkt gegevens over de gezondheid in het kader van aftrek van zorgkosten en over lidmaatschap van vakbond of kerkgenootschappen in het kader van de giftenaftrek in het kader van de inkomstenbelasting. Op grond van artikel 30 van de Uitvoeringswet AVG is dit toegestaan indien dit nodig is ten behoeve van de uitvoering van wettelijke voorschriften. Deze gegevens worden niet herkenbaar vastgelegd in ABS (dat wil zeggen: alleen de bedragen van de kosten en giften zijn opgenomen, niet de precieze herkomst of bestemming). Ook worden gezondheidsgegevens verwerkt in het kader van de BPM (ontheffing voor motorrijtuigen voor gehandicapten).

Als werkgever verwerkt de Belastingdienst uiteraard ook gegevens over gezondheid op grond van bijvoorbeeld ziekmeldingen, in aangelegenheden rond arbeidsomstandigheden of in het kader van beschikbaarstelling van invalideparkeerplaatsen. Het omgaan met dergelijke bijzondere gegevens is door de AP al onder de Wbp geprotocolleerd. Wat wel en niet is toegestaan is door (de voorloper van) de concerndirectie O&P in de organisatie kenbaar gemaakt via een ManagementUpdate. Dat iemand ziek is mag natuurlijk worden gemeld, maar verder moet zeer terughoudend worden omgegaan met dergelijke informatie.

Geen beslispunt

3.2.4 Strafrechtelijke gegevens
In artikel 10 wordt de verwerking van strafrechtelijke gegevens geregeld, eveneens als uitwerking van het beginsel van *rechtmatigheid*. Deze gegevens mogen alleen worden verwerkt onder toezicht van de overheid, of indien de verwerking is toegestaan bij nationaal recht.

In de artikelen 31 tot en met 33 van de Uitvoeringswet AVG is een nationale regeling getroffen voor deze gegevens. Hierin is geregeld dat strafrechtelijke gegevens mogen worden verwerkt door organen die deze hebben verkregen op grond van de Wet politiegegevens. Dit geldt voor de FIOD. De verwerking van strafrechtelijke gegevens wordt voor het overige gereguleerd door de Richtlijn

(strafrechtelijke gegevens) die geïmplementeerd is in de Wet politiegegevens. Deze wordt ook van toepassing op de buitengewone opsporingsambtenaren bij de Belastingdienst en bij Douane. Dit heeft impact voor de organisatie en systemen van deze dienstonderdelen; deze worden op dit moment in kaart gebracht.

Geen beslispunt

3.2.5 Rechten van betrokkenen
De artikelen 15 tot en met 21 regelen de recht van betrokkene ten aanzien van zijn persoonsgegevens. Het gaat hier om het recht van inzage, van correctie, van vergetelheid, van overdraagbaarheid, van beperking van de verwerking en van bezwaar tegen de verwerking.

Het proces voor het behandelen van inzageverzoeken wordt op dit moment ingericht, waarbij rekening wordt gehouden met een (in de beginfase aanzienlijke) toename van de inzageverzoeken. Het DT heeft op 29 maart ingestemd met dit proces. Via Switch is een beperkt aanbod van capaciteit beschikbaar om indien nodig te kunnen opschalen. Met CAP zijn afspraken gemaakt over tijdelijke inzet van capaciteit.
Op de privacypagina op de website zal expliciet aandacht worden besteed aan de reguliere mogelijkheden om gegevens te wijzigen, zodat extra belasting van het inzage/correctieproces wordt voorkomen.
De rechten op vergetelheid en overdraagbaarheid van gegevens gelden niet indien de verwerking van de gegevens noodzakelijk is voor de vervulling van een wettelijke taak van algemeen belang. Dit betekent dat deze voor de Belastingdienst met name relevant zijn voor zover het verwerking van persoonsgegevens in het kader van bedrijfsvoering betreft. Voor personeelsgegevens worden deze rechten (deels) ondersteund via P-Direkt. Het recht van vergetelheid kan voor gegevens uit primaire processen wel worden ingeroepen in geval de gegevens langer bewaard worden dan noodzakelijk is voor de uit te voeren taken. Een goed schoningsbeleid (zie 3.1.1) zal het beroep op dit recht minimaliseren.
Het behandelen AVG-bezwaar tegen de verwerking van gegevens geschiedt op dezelfde manier als van inzage- en correctieverzoeken.

Indien gegevens zijn gecorrigeerd, moeten eventuele afnemers van de correctie op de hoogte worden gesteld. De Belastingdienst levert aan afnemers altijd actuele gegevensbestanden. Bij de eerstvolgende levering wordt een eventueel gecorrigeerd gegeven geleverd. Het apart informeren van de afnemers is daardoor niet nodig. Dit zou alleen anders kunnen zijn in geval van een eenmalige levering van gegevens voor langdurig gebruik. Bezien moet worden of deze situatie zich voordoet.
De genoemde rechten kunnen (net als de informatieplicht uit artikel 13 en 14) worden ingeperkt. Dit is toegelicht in paragraaf 3.1.5.

Beslispunten

Beleidslijnen
ll. De rechten van vergetelheid en overdraagbaarheid van gegevens zijn met name relevant voor persoonsgegevens die in het kader van de bedrijfsvoering worden verwerkt. Beroep op het recht van vergetelheid ten aanzien van gegevens in primaire processen wordt geminimaliseerd door een goed schoningsbeleid.
mm. Afnemers van gegevens worden niet expliciet geïnformeerd over wijzigingen in de gegevens op grond van een toegekend verzoek tot correctie; de gecorrigeerde gegevens worden meegeleverd in de eerstvolgende levering.

Bij een eenmalige levering voor langdurig gebruik kan informeren van de afnemer wel wenselijk zijn.

Actie
nn. Het proces voor behandeling van inzageverzoeken wordt ingericht conform het besluit van het DT van 29 maart 2018, waarbij rekening wordt gehouden met een aanzienlijke toename van het aantal verzoeken in de eerste maanden na 25 mei 2018.
oo. De dienstonderdelen brengen in kaart of eenmalige leveringen voorkomen, met het oog op informeren van de afnemer over correcties.

3.2.6 Gezamenlijke verwerkingsverantwoordelijkheid

Artikel 26 bevat een regeling indien twee of meer partijen gezamenlijk als verwerkingsverantwoordelijke zijn aan te merken. Zij moeten dan hun respectieve verantwoordelijkheden ten aanzien van de nakoming van de verordening vastleggen, en ten aanzien van de uitoefening van de rechten van betrokkenen.

Voor de Belastingdienst is deze bepaling relevant bij gegevensuitwisseling in samenwerkingsverbanden zoals RIEC/LIEC, LSI, FEC en iCOV. De verstrekking van gegevens aan (deelnemers aan) samenwerkingsverbanden geschiedt op basis van doorbreking van de geheimhouding (zie hierboven bij artikel 6). De daarbij geldende voorwaarden – waaronder het in acht nemen van de privacywetgeving door de wederpartij – worden neergelegd in convenanten.
Het Ministerie van J&V werkt aan een wetsvoorstel gegevensuitwisseling in samenwerkingsverbanden, waarin een basis wordt gecreëerd voor het delen van gegevens in samenwerkingsverbanden, op grond van bij amvb te stellen regels. Het wetsvoorstel is afgestemd op de AVG. Indien een samenwerkingsverband waarin de Belastingdienst participeert te zijner tijd onder deze wetgeving wordt gebracht, zal ook de uitwerking van gezamenlijke verwerkingsverantwoordelijkheid in de desbetreffende amvb worden geregeld.

Geen beslispunt

3.2.7 Verwerkingenregister

Artikel 30 bevat de verplichting om een register van verwerkingsactiviteiten bij te houden ten behoeve van het toezicht. Dit geeft nader invulling aan de *verantwoordingsplicht*.

De realisering van het AVG-register door de Belastingdienst is afgerond. Een aantal verwerkingen wacht nog op review en goedkeuring door de FG.
Het beheer van het register is deels ingevuld. De datacoördinatoren van de onderdelen zorgen dat nieuwe verwerkingen en uitgevoerde PIA's in het register worden opgenomen. De rol van de concerndirectie IV&D bij het beheren van het register wordt meegenomen bij inrichting van deze directie, evenals de wijze waarop IV&D zijn controlfunctie ten aanzien van geregistreerd PIA's en de naar aanleiding daarvan te nemen maatregelen uitvoert. Omdat een en ander strikt genomen op 25 mei operationeel moet zijn, kan niet worden gewacht tot formele afronding van het formele inrichtingsproces van IV&D, maar moeten tijdelijke werkverbanden worden georganiseerd.

Beslispunt

Actie
pp. Onder de verantwoordelijkheid van de km/bd IV&D wordt, vooruitlopend op de afronding van een formele inrichting van de concerndirectie IV&D, een tijdelijk werkverband en tijdelijke capaciteit georganiseerd om de voortgang van AVG-gerelateerde taken per 25 mei 2018 te verzekeren.

3.2.8 Meldplicht datalekken

In artikel 33 is de meldplicht datalekken geregeld, als uitwerking van de beginselen van *rechtmatigheid*, *behoorlijkheid* en *transparantie*, en ook *integriteit* en *vertrouwelijkheid*.

Het proces voor melding van datalekken is al ingericht op basis van de verplichtingen hiertoe in de Wbp. Dit proces is geactualiseerd op grond van de AVG. De procedurebeschrijving is bijgevoegd ter accordering. De directie IV&D vervult een coördinerende en controlerende rol bij de melding van datalekken. Deze moet bij de inrichting van deze directie verder worden ingevuld.

Beslispunt

qq. Het DT stelt de geactualiseerde procedure melding datalekken vast.

3.2.9 Raadpleging AP na PIA

Artikel 36 vereist dat in geval een PIA is gemaakt die risico's laat zien ten aanzien van een gegevensverwerking, maar de te nemen maatregelen niet gerealiseerd kunnen worden, de AP wordt geraadpleegd over de voorgenomen verwerking. Dit is een uitwerking van de verantwoordingsplicht en voorts van de beginselen van *rechtmatigheid*, *integriteit* en *vertrouwelijkheid*.

In het proces van uitvoeren van een PIA zelf moet advies worden gevraagd aan de FG. Beide verplichtingen worden opgenomen in de Handleiding uitvoeren PIA's, waarvan het DT op 26 april een conceptversie heeft geaccordeerd.

Geen beslispunt

3.2.10 Aanwijzen Functionaris gegevensbescherming

Artikel 37 verplicht tot het aanwijzen van een Functionaris gegevensbescherming die optreedt als interne toezichthouder op naleving van de AVG. Hiermee wordt de *verantwoordingsplicht* ondersteund.

Bij Financiën was al een FG aangesteld, deze zal zijn werkzaamheden onder de AVG voortzetten. Het DT heeft op 29 maart ook ingestemd met een voorstel voor het inrichten en formaliseren van de privacyfunctie binnen de Belastingdienst. Met implementatie daarvan is een start gemaakt, door het beschikbaar stellen van een rolbeschrijving voor datacoördinatoren bij alle dienstonderdelen. Zij hebben op basis daarvan deze rol toebedeeld aan bestaande functionarissen (bv. in de vaktechnische infrastructuur) of een belangstellingsregistratie uitgezet. De datacoördinatoren vormen de eerste laag in de privacy-infrastructuur bij de Belastingdienst. Zij kunnen bij hun werkzaamheden (oa. ondersteuning bij PIA's, beheer AVG-register, vraagbaakfunctie) hulp inroepen bij CAP (team juridische advies gegevens). Dit is de tweede laag in de infrastructuur. De derde laag wordt gevormd door de concerndirectie IV&D, die tevens als centraal aanspreekpunt fungeert voor de FG.

Beslispunt

Actie

rr. Alle bedrijfsonderdelen dragen zorg voor de verdere inrichting van de privacyfunctie conform het daarvoor door het DT geaccordeerde voorstel (besluit DT van 29 maart 2018).

Bijlage

Hieronder volgt een overzicht van de acties uit dit document. Er kunnen meer acties lopen, die vanuit de directies zelf zijn of worden opgepakt.

Actie#	Omschrijving	Wie
1	Bespreken risico analyses en maatregelen aan ketentafels en in onderdeel MT's	Alle bedrijfsonderdelen
2	N.a.v. bespreking risico's maatregelen doorvoeren in IV portfolio via ketentafels	Alle bedrijfsonderdelen
3	Niet archiefwaardige bestanden vernietigen	Alle bedrijfsonderdelen
4	Actualiseren selectielijsten o.l.v. SSO CFD	Alle bedrijfsonderdelen
5	Toepassen selectielijsten; archiefwaardige bestanden overbrengen naar archief, schonen bestaande systemen	Alle bedrijfsonderdelen
6	Definiëren kwaliteitsmaatregelen register, maken auditplan	CD IV&D
7	Doorvoeren kwaliteitsverbetering van het AVG register o.l.v. IV&D	Alle bedrijfsonderdelen
8	Kaders ontwikkelen voor beperken van rechten van betrokkenen iom FJZ en IV&D	CD UHB
9	Afspraken maken met DGFZ over het uitvoeren van PIA's in voorbereidingsfase wetgeving	CD UHB
10	Opnemen van PbDD in architectuurkaders, waar ontwerpproducten aan worden getoetst	CD IV&D
11	Uitwerken van PbDD in concrete voorschriften voor ontwerp van processen en IV-voorzieningen	IV
12	Afsluiten of actualiseren verwerkersovereenkomsten	Alle bedrijfsonderdelen
13	opstellen interne gegevens leveringen ovk's	CAP/BICC
14	Wmk toets uitvoeren voor alle interne gegevensverstrekkingen	Alle bedrijfsonderdelen
15	Uitfaseren wisselland	CAP/BICC
16	Uitfaseren datadumping faciliteiten dan wel gebruik afschermen	IV
17	gebruik productiedata in testomgeving stoppen; pseudonimiseren dan wel fictieve testdata gebruiken	IV
18	Beoordelen actualiteit van toegekende autorisaties, ondersteund door F&MI	Alle bedrijfsonderdelen
19	Uitwerken beleids- en ontwerpprincipes vernieuwd autorisatiebeleid i.s.m. F&MI	CD IV&D
20	In beeld brengen verwerkingen personeelsgegevens inclusief beoordeling van noodzaak, namens CD O&P	SSO O&P
21	Rationalisatie LOA's in bedrijfsvoeringsprocessen die personeelsgegevens verwerken, namens CD O&P	SSO O&P
22	Heroriëntatie op het applicatielandschap, dominante positie P-Direkt t.a.v. beheer personeelsgegevens	CD O&P ism SSO O&P
23	Heldere afbakening van verantwoordelijkheden tussen CAP, F&MI, DF&A en IV m.b.t. gegevensverwerking	Ketendirecteur Gegevens
24	Kaders uitwerken voor de waarborgen in het bijzondere geval dat testen met productiedata toch nodig is, i.s.m. IV en CAP	CD IV&D
25	toeslagen uitwisseling DUO/UWV grondslag bespreken met DGFZ	Toeslagen
26	beoordelen proportionaliteit inwinnen gegevens	CAP
27	PIA's uitvoeren op gegevensverwerkingen conform handleiding PIA proces	Alle bedrijfsonderdelen

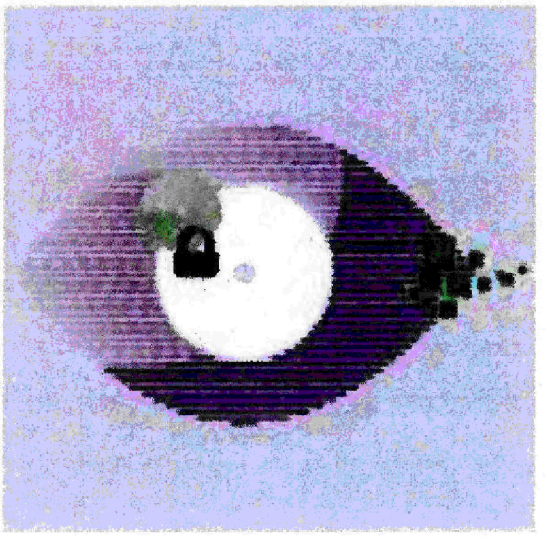
28	Beoordelen (web)formulieren op proportionaliteit door documenteigenaar	Alle bedrijfsonderdelen
29	Beoordeling van bilaterale verdragen op buiten EU op vergelijkbaar beschermingsniveau laten verrichten door DGFZ	CD UHB
30	Advies om beslisregels transparant te maken	IV
31	Herstel van grondslag voor verwerking van personeelsgegevens Shuttelkaart aankaarten bij BZK i.s.m. CD O&P	SSO CFD
32	Overleg m.b.t. (tussen)oplossingen IB-47 proces met DGFZ	CD UHB
33	Kaderstelling noodzaak gegevensverwerking o.b.v. toestemming en o.b.v. gerechtvaardigd belang	CD IV&D
34	In kaart brengen incidentele externe gegevensleveringen i.v.m. informeren over correcties	Alle bedrijfsonderdelen
35	Voorziening realiseren t.b.v. toestemming gebruik telefoonnummer t.b.v. dienstverlening	KI&S
36	Inrichting controle op aangifte IH van iedere Belastingdienst medewerker vanwege integriteit (ambtenarentabel) met FJZ	Programma AVG
37	Tijdelijk werkverband organiseren als transitieorganisatie	CD IV&D
38	Verdere inrichting van de privacy functie (zoals aanstellen datacoördinator, organiseren netwerk)	Alle bedrijfsonderdelen

bylage 2

Belastingdienst

Eindrapport programma AVG

Implementatie
Algemene Verordening Gegevensbescherming
AVG



Colofon

Titel	Eindrapport programma AVG
Versienummer	1.0
Datum definitief	19 juli 2018
Documentlocatie	Programmadossier
Programmamanager	Persoonsgegevens

Inhoud eindrapport programma AVG

1 Documenteigenschappen

1.1 Historie

Versie	Datum	Veranderingen (concept/definitief)	Auteur(s)
0.1	18-06-2018	Concept	Persoonsgegevens
0.2	22-06-2018	Concept	
0.5	28-06-2018	Concept	
0.8	03-07-2018	Concept, reviewopmerkingen Persoonsgegevens verwerkt	
1.0	19 juli 2018	Conform versie 0.8 definitief gemaakt	

1.2 Distributie

De volgende personen hebben een exemplaar ontvangen.

Naam	Rol	Datum document	Versie
Kernteamleden AVG		18 juni 2018	V0.1
Programmamanager		22 juni 2018	V0.2
Persoonsgegevens	Opdrachtgever	28 juni 2018	V0.5
	Opdrachtgever	03 juli 2018	V0.8
Beschikbaar	Beschikbaar	19 juli 2018	V1.0

2 Doel eindrapport programma AVG

Dit eindrapport beschrijft de resultaten behaald met de implementatie van de Algemene Verordening Gegevensbescherming (AVG) per 25 mei 2018, de overdracht van het programma AVG naar de nieuwe concerndirectie IV en Databeheersing (IV&D) en andere bedrijfsonderdelen, inzicht in het vervolgtraject en de afhandeling van openstaande acties.

Het Directieteam (DT) van de Belastingdienst heeft op 19 juli 2018 decharge verleend aan het programma AVG met terugwerkende kracht per 1 juli 2018. Het programma AVG is daarmee ontbonden. Deze versie van het eindrapport is inhoudelijk ongewijzigd ten opzichte van de aan het DT BD opgeleverde eindrapport, versie 0.8. Hiermee heeft het eindrapport programma AVG een definitieve status verkregen.