Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Aanvullend onderzoek AVG - Belastingdienst

Definitief

Colofon

Titel	Aanvullend onderzoek AVG - Belastingdienst
Uitgebracht aan	Directeur-Generaal Belastingdienst, dr. J.J.M. Uijlenbroek
Datum	20 december 2019
Kenmerk	2019-0000212883

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Op verzoek van de plaatsvervangend secretaris-generaal heeft de ADR begin 2019 onderzoek gedaan naar de stand van zaken van een aantal maatregelen uit de implementatieplannen aangaande de Algemene Verordening Gegevensbescherming (AVG) binnen het Ministerie van Financiën. Dit heeft geresulteerd in een rapport met kenmerk 2019-0000062907, waarbij de peildatum van het onderzoek 28 februari 2019 was.

In de brief van de staatssecretaris aan de Tweede Kamer, d.d. 28 mei 2019 is het volgende gesteld:

> *De periode februari-mei 2019 heeft de Belastingdienst gebruikt om de bevindingen van de ADR weg te nemen. De Belastingdienst meldt dat de bevindingen inmiddels zijn opgelost, met uitzondering van het verwijderen van oude gegevens*
>
> *Om de uitvoering van de aanbevelingen door de Belastingdienst te toetsen, zal ik de ADR vragen een aanvullende audit te doen op de implementatie van de AVG bij de Belastingdienst. De uitkomst van de aanvullende audit zal ik te zijner tijd aan uw Kamer te sturen.*[1]

Dit rapport geeft de uitkomsten van het aanvullende onderzoek weer.

Belastingdienst is aan de slag gegaan met aanbevelingen, maar bevindingen zijn nog niet volledig weggewerkt

De Belastingdienst is aan de slag gegaan met de ADR-aanbevelingen (zie hoofdstuk 1):

- De heroverweging van AVG-acties is uitgevoerd;
- De regie op belastingdienstbrede AVG-acties staat in de steigers;
- Een eerste aanzet voor een pro-actievere rol van de privacyofficer/IV&D is gegeven;
- IV&D werkt aan het opstellen van enkele uitvoeringsrichtlijnen;
- Structurele verbeteracties belegd in de lijn;
- De Belastingdienst heeft een start gemaakt met de overige aandachtspunten.

De ADR-bevindingen zijn nog niet geheel weggewerkt (zie hoofdstuk 2):

- De realisatie van de intrekkingsactie van segmentvreemde rollen bij CAP en MKB op hoofdlijnen navolgbaar;
- Structurele verbeterslag autorisaties heeft de aandacht, belastingdienst-brede afstemming is nodig;
- Alle Belastingdienst applicaties zijn geïnventariseerd op de aanwezigheid van een bulk-export functie. Structurele afhandeling van deze lijst is niet aangetroffen;
- Geen voortgang op registratie van verwerkersovereenkomsten in AVG-register;
- Uitwerking beleid 'geen productiedata in test' in werkinstructies nog niet beschikbaar.

---

[1] Deze passage is 1 op 1 overgenomen uit de brief van 28 mei 2019 van de staatssecretaris aan de Tweede Kamer; Kamerstukken II 2018/19, 31 066, nt 485

De centrale boodschap is dat de Belastingdienst met de aanbevelingen aan de slag is gegaan, maar dat er nog vervolgacties nodig zijn om alle bevindingen volledig op te lossen (zie hoofdstuk 3). Tenslotte geven we in hoofdstuk 4 nadere toelichting op de opzet en uitvoering van dit onderzoek.

1 De Belastingdienst is aan de slag gegaan met de ADR-aanbevelingen

1.1 Heroverweging van AVG-acties is uitgevoerd

Achtergrond van de ADR-aanbeveling uit het initiële rapport om een herover-weging te doen van alle issues (AVG acties) was om enerzijds zeker te zijn dat deze acties noodzakelijk zijn voor het aantoonbaar voldoen aan de AVG. Anderzijds om vast te stellen dat de eerder onderkende risico's door de voorgestelde AVG-acties op een zo effectief mogelijke wijze worden afgedekt en dat er geen betere alternatieven voorhanden zijn. Tenslotte dient het te bereiken doel voor elke AVG-actie heel concreet te worden uitgewerkt om daadwerkelijk te kunnen meten of het doel op 25 mei 2019 is gehaald.

Uit ons onderzoek blijkt dat een heroverweging van de generieke maatregelen is uitgevoerd en vastgelegd door IV&D. De heroverweging van de dienstonderdeel specifieke maatregelen is door de dienstonderdelen zelf uitgevoerd. De resultaten van de AVG-acties zijn vastgelegd in de eindrapportages per dienstonderdeel.
De vastlegging van de uitkomst van de heroverweging van de acties die een andere aanpak hebben gekregen, is meestal vastgelegd in de trant van 'zal worden opgepakt in de reguliere lijn'.

1.2 Regie op belastingdienstbrede AVG-acties staat in de steigers

Achtergrond van de ADR-aanbeveling uit het initiële rapport om een meer projectmatige aanpak toe te passen was om strakker te kunnen sturen op tijdige realisatie van de AVG-acties met als doorlooptijd 25 mei 2019. Dit betekent dat er meer regie op de uitvoering is door de data-coördinatoren en dat er, indien nodig, sneller bijgestuurd kan worden. Wij denken hierbij dat een model met decentrale projectleiders die worden ondersteund door een centraal projectbureau, het best aansluit bij de huidige besturingsfilosofie van de Belastingdienst. Wij benadrukken hierbij het feit dat de projectleiders voldoende inhoudelijke expertise dienen te hebben.

Uit ons onderzoek van september/oktober 2019 blijkt dat de implementatie van de AVG-acties vanaf 25 mei 2019 volledig in de lijn is belegd. CAP heeft een check uitgevoerd en vastgelegd om vast te stellen dat inderdaad alle AVG-acties nu in de lijn zijn belegd.

In ons onderzoek zijn we de volgende belastingdienstbrede thema's tegengekomen:
- Schonen van persoonsgegevens;
- Het volledig vullen van, en een kwaliteitsslag op, het AVG-register;
- Structurele andere opzet autorisatiebeheer mede als gevolg van nieuwe topstructuur.

De kaderstelling ligt bij de concerndirectie IV&D. Op dit moment ondersteunt IV&D ook bij de implementatie van de kaders, bijvoorbeeld door workshops te organiseren hoe de directies dienen om te gaan met de Datakluis[2]. In het datacoördinatorenoverleg wordt een vaste tijd van het overleg ingepland om issues met betrekking tot de implementatie van deze belastingdienstbrede thema's af te stemmen tussen de verschillende dienstonderdelen.

[2] Een datakluis is een afgeschermd opslaggebied waarin bestanden -al dan niet met persoonsgegevens- die ouder zijn dan een vooraf bepaalde leeftijd geplaatst zijn. Bestanden in de datakluis zijn niet toegankelijk voor gebruikers. Alleen een kluisbeheerder kan besluiten een onterecht naar de datakluis verplaatst bestand terug te zetten.

Door een goede afstemming kan de voortgang van de implementatie van deze thema's bespoedigd worden evenals een uniforme uitwerking binnen de gehele Belastingdienst.

1.3 Eerste aanzet voor een pro-actievere rol privacyofficer/IV&D is gegeven

Achtergrond van de ADR-aanbeveling uit het initiële rapport is dat de ADR weinig ondersteuning van de belastingdienstonderdelen aantrof op het gebied van de AVG. Daarom was de aanbeveling om de CIO Office Belastingdienst en dan met name de privacyofficer een pro-actieve rol toe te delen in het ondersteunen van de datacoördinatoren.

Uit ons onderzoek blijkt dat de privacyofficer (PO) invulling heeft gegeven aan een pro-actievere rol door periodiek overleg te hebben met de datacoördinatoren (DC-en) in een DC-overleg. Uit de verslagen van de DC-overleggen zien we veel goede initiatieven, maar naar ons idee is de voortgang op de verschillende onderwerpen niet zo groot. Wellicht veroorzaakt doordat erbij de datacoördinatoren onduidelijkheid is over de interpretatie van de huidige rolbeschrijving.
NB: De lijndirecteuren zijn verantwoordelijk voor de implementatie van de AVG, niet de datacoördinatoren.

De PO heeft het voornemen om samen met de Functionaris Gegevensbescherming (FG) regelmatig de verschillende dienstonderdelen te bezoeken. De afspraken hiervoor zijn nog niet gepland.

1.4 IV&D werkt aan het opstellen van enkele uitvoeringsrichtlijnen[3]

Achtergrond van de ADR-aanbeveling uit het initiële rapport is dat er binnen de Belastingdienst nog niet veel ervaring is opgedaan met de nieuwe topstructuur, gebaseerd op een scheiding tussen beleid en uitvoering. Ons advies was om voor wat betreft de AVG de beleidskaders (ofwel uitvoeringsrichtlijnen) te laten opstellen in nauwe samenwerking met de uitvoerende belastingdienstonderdelen.

Uit ons onderzoek blijkt dat IV&D momenteel werkt aan 4 verschillende uitvoeringsrichtlijnen:

- uniformeren procedure datalekken;
- proces van formalisering GEB/DPIA's (Gegevensbeschermingseffect-beoordeling/Data protection impact assessment);
- werkwijze vullen van verwerkingsregister;
- een rijksbreed te gebruiken normenkader voor privacy onder coördinatie van het ministerie van Justitie en Veiligheid.

De behoefte aan andere uitvoeringsrichtlijnen wordt besproken in het DC-overleg, voorgezeten door de PO. In dit gremium zijn alle belastingdienstonderdelen vertegenwoordigd.

In het initiële onderzoek van de ADR zijn de volgende uitvoeringsrichtlijnen genoemd:

- uitgangspunten bij toepassing selectielijsten;
- uitgangspunten vernietiging bestanden op samenwerkingsgebieden;
- verantwoordelijkheidsverdeling van de dienstonderdelen bij gebruik gegevens in een keten;
- uitgangspunten bepaling noodzaak maken verwerkersafspraken.

Op bovenstaande punten hebben wij nog geen voortgang kunnen vaststellen. De mogelijkheid voor IV&D om aan het opstellen van uitvoeringsrichtlijnen te werken wordt overigens sterk bepaald door het grote beslag dat de actualiteit op de afdeling legt, zoals het beantwoorden van Kamervragen en vragen van toezichthouders als

[3] In het initiële onderzoek werden de uitvoeringsrichtlijnen beleidskaders genoemd.

de AP[4], de ADR[5] en de ARK[6] en van (externe) commissies als de "Adviescommissie uitvoering toeslagen". Het werken aan structurele verbeteracties komt hierdoor in de verdrukking.

1.5 Structurele AVG-verbeteracties belegd in de lijn

Achtergrond van de ADR-aanbeveling uit het initiële rapport is om de structurele verbeteracties die van belang zijn voor de naleving van de AVG, maar in feite een breder bereik hebben, op te nemen in een separaat project en dit belastingdienstbreed af te stemmen en hier ook een projectmatige aanpak op te zetten.

Dit betreft in ieder geval de volgende onderwerpen:
- *de implementatie van de selectielijsten;*
- *het op orde brengen van de informatiehuishouding (bijvoorbeeld langs de lijnen van het 'Rijksprogramma voor Duurzaam Digitale Informatiehuishouding').*

MKB en CAP hebben aandacht voor structurele verbeteracties. Dit komt tot uiting in (implementatie)plannen om AVG-aspecten in de lijn te borgen. Het plan van CAP om AVG in de lijn te borgen is vastgesteld in het MT van CAP op 2 september 2019.
De regie op belastingdienstbrede structurele AVG-verbeteracties ligt bij IV&D, zie ook paragraaf 1.2.
De reguliere monitoring gebeurt via de Viermaandsrapportage (VMR) op basis van kaderstelling IV&D en mede via de 2de lijns control-functie bij de diverse dienstonderdelen. De reguliere monitoring inzake de AVG viel buiten de scope van dit onderzoek.

1.6 De Belastingdienst heeft een start gemaakt met de overige aandachtspunten

Achtergrond hiervan is dat uit het initiële ADR-onderzoek nog een aantal aandachtspunten naar voren kwamen die van belang zijn voor de aantoonbare naleving van de AVG. Het advies was om structureel aandacht te geven aan:
- *het verbeteren van het inzicht in het gebruik van persoonsgegevens in de keten;*
- *het zodanig managen van de prioriteitstelling in de IV dat de functionaliteiten t.b.v. schonen na verstrijken bewaartermijnen in de applicaties kunnen worden aangebracht;*
- *het ontwikkelen van een voldoende dekkend AVG-normenkader om AVG-toetsing beter mogelijk te maken.*

<u>Verbeteren van inzicht in het gebruik van persoonsgegevens in de keten</u>
Met een GEB/DPIA worden de gebruikte persoonsgegevens binnen een keten in kaart gebracht. De Belastingdienst heeft een conceptprocedure voor het uitvoeren van een GEB/DPIA met als naam "Handleiding Gegevensbeschermingseffect-beoordeling (GEB/DPIA) Belastingdienst". Deze procedurebeschrijving is een aanvulling op de handreiking van het Ministerie van JenV en de procedure van het kerndepartement, maar dan toegespitst op de Belastingdienst. De procedure is een 0.2 versie en moet nog worden geformaliseerd. De datacoördinatoren hebben opmerkingen ingebracht. De opmerkingen worden nu beoordeeld en verwerkt. Daarna volgt een nieuwe afstemronde.

[4] AP = Autoriteit persoonsgegevens
[5] ADR = Auditdienst Rijk
[6] ARK = Algemene Rekenkamer

Managen prioriteitstelling inzake schoningsfaciliteiten
Er is een lijst met applicaties waarop is aangegeven of er in de applicatie schoningsfaciliteiten aanwezig zijn. Onduidelijk is hoe deze lijst wordt beheerd.

Binnen de Belastingdienst bestaat een checklist voor procesontwerpers uit 2014. Hierbij is de volgende vraag opgenomen met betrekking tot gegevens: "Zijn de lifecycle aspecten beschreven (conversie, bewaartermijnen en schoning)?".
Dit betekent dat in opzet bij de ontwikkeling van nieuwe applicaties aandacht wordt gevraagd voor schoningsfaciliteiten. Een beoordeling of deze checklist ook bij de ontwikkeling van alle Belastingdienst applicaties wordt gebruikt en of hierop wordt getoetst, viel buiten de scope van het onderzoek.

Ontwikkelen voldoende dekkend AVG-normenkader
Het ministerie van Justitie en Veiligheid (JenV) is samen met een interdepartementale schrijfgroep gestart om een rijksbreed te gebruiken AVG-normenkader op te stellen. Zowel de privacyofficers van de Belastingdienst als van het kerndepartement Financiën zijn hierbij betrokken.
Momenteel wordt gewerkt aan een handreiking. Het streven is om deze op korte termijn te voltooien voor afstemming. In 2020 zal de handreiking (als groeimodel) verder worden uitgewerkt tot normenkader.

2 ADR-bevindingen nog niet volledig weggewerkt

2.1 Realisatie intrekkingsactie segmentvreemde rollen bij CAP en MKB op hoofdlijnen navolgbaar

ADR-bevinding uit het initiële rapport: Maatregel inzake intrekken autorisaties is alleen haalbaar voor dienstonderdeelvreemde rollen

MKB
Wij hebben kunnen vaststellen dat MKB alle rollen heeft beoordeeld en dat de bijbehorende intrekkingsactie wordt uitgevoerd. De processtappen zijn op hoofdlijnen te volgen, maar niet op een cijfermatige wijze.
Reden hiervoor is dat geen mutatie-overzicht is bijgehouden van de verschillende stappen. Het eindresultaat is per april/mei 2019 beoordeeld, hieruit bleek een significante daling van segmentvreemde rollen. Van ongeveer 500 rollen (+/- 2%) moet nog bepaald worden welke vervolgactie (handhaven, toevoegen aan andere bedrijfsrol of intrekken) plaats moet vinden.

CAP
Wij hebben kunnen vaststellen dat CAP alle segmentvreemde rollen heeft beoordeeld voor mei 2019 en dat de bijbehorende intrekkingsactie wordt uitgevoerd. De nog niet geschoonde segmentvreemde rollen en de CAP rollen worden in de 2e helft van 2019 beoordeeld en indien nodig ingetrokken. De processtappen zijn te volgen, maar niet op een cijfermatige wijze.
Reden hiervoor is dat geen mutatie-overzicht is bijgehouden. Wel heeft FM&I CAP per mail décharge verleend voor de intrekkingsactie. Het eindresultaat is per 25 mei 2019 beoordeeld, hieruit bleek een significante daling van segmentvreemde rollen. Van ongeveer 700 rollen (+/- 5%) moet nog bepaald worden welke vervolgactie (handhaven, toevoegen aan andere bedrijfsrol of intrekken) plaats moet vinden.

2.2 Structurele verbeterslag autorisaties heeft de aandacht, belastingdienst-brede afstemming is nodig

ADR-bevinding uit het initiële rapport: Structurele verbeterslagen in autorisatiebeheer vragen een langere doorlooptijd

MKB heeft een concept-verbeterplan opgesteld voor het structureel verbeteren van het inrichten en beheer van de autorisaties.
CAP heeft een analyse van alle thema's/issues gemaakt ten behoeve van de governance rondom de structurele verbeterslagen en alles belegd in de lijn om deze punten op te lossen.

Aandachtspunt hierbij is dat er belastingdienstbrede kaders moeten komen om een meer uniforme opzet van de bedrijfsrollen te realiseren. Hiervoor is afstemming nodig tussen alle belastingdienstonderdelen.

2.3 Alle Belastingdienst applicaties zijn geïnventariseerd op de aanwezigheid van een bulk-export functie. Structurele afhandeling van deze lijst is niet aangetroffen.

ADR-bevinding uit het initiële rapport: Maatregel inzake datadumping faciliteiten (bulk-export functies) uitfaseren dan wel afschermen is niet voldoende SMART gemaakt

Alle Belastingdienst applicaties zijn door directie IV geïnventariseerd op AVG-issues. Onduidelijk is in hoeverre alle Belastingdienst applicaties op het aspect 'het hebben van een bulk-export functie' zijn beoordeeld. Met andere woorden, wij hebben de volledigheid van de inventarisatielijst niet kunnen vaststellen. Daarnaast hebben wij de afhandeling van deze lijst niet aangetroffen waardoor onduidelijk is of er acties zijn ondernomen n.a.v. de inventarisatie.

2.4 Geen voortgang op registratie van verwerkersovereenkomsten in AVG-register[7]

ADR-bevinding uit het initiële rapport: Nog niet alle verwerkersovereenkomsten zijn aanwezig of geactualiseerd

Uit de analyse van begin september 2019 blijkt dat er geen voortgang is geboekt ten opzichte van februari 2019 met betrekking tot de volledigheid en de actualiteit van de registratie van verwerkersovereenkomsten in het AVG-register van het Ministerie van Financiën.

2.5 Uitwerking beleid 'geen productiedata in test' in werkinstructies nog niet beschikbaar

ADR-bevinding uit het initiële rapport: Maatregel 'gebruik productiedata in testomgeving stoppen' is niet voldoende SMART gemaakt

In de notitie "AVG: beleidslijnen en acties geconsolideerd" van juli 2018 wordt aangegeven dat het testen van systemen dient te geschieden met fictieve testdata dan wel met gepseudonimiseerde productiegegevens.
In het verslag Directieteam Belastingdienst van 24 mei 2018 staat inzake het gebruik van productiedata in test de volgende beleidslijn geformuleerd:

> *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.*

Tijdens het onderzoek hebben wij geen uitwerking van deze beleidslijnen aangetroffen. Over de uitwerking van het beleid in werkinstructies wordt in de ketentafel Gegevens gesproken door CAP en IV.

[7] Met het AVG-register wordt bedoeld het verwerkingsregister zoals door het ministerie van Financiën wordt gebruikt.

3 Vervolgstappen

De Belastingdienst is met de ADR-aanbevelingen aan de slag gegaan, maar het is belangrijk dat hierop wordt doorgepakt:

- Voor het structureel voldoen aan de AVG staan een aantal belangrijke acties gepland. Wij willen hier benadrukken dat met name een volledige vulling van alle velden in het AVG-register en een kwaliteitsverbetering van het AVG-register een belangrijke stap is om invulling te geven aan de Informatieplicht conform de AVG;
- IV&D werkt aan een aantal uitvoeringsrichtlijnen. Het is belangrijk dat voldoende capaciteit beschikbaar komt, zodat de onderhanden uitvoeringsrichtlijnen snel gerealiseerd kunnen worden en dat gestart kan worden met nieuwe uitvoeringsrichtlijnen;
- We zien een pro-actievere rol van de privacyofficer. Door periodiek al dan niet met de functionaris gegevensbescherming een rondje langs de verschillende dienstonderdelen te maken, kan dit nog versterkt worden. Onduidelijkheid over de interpretatie van de huidige rolbeschrijving van de datacoördinatoren kan worden opgelost door een evaluatie en eventuele actualisatieslag van deze rolbeschrijving.

De ADR-aanbeveling "Heroverweging van AVG-acties" Is gerealiseerd. Hiervoor is een vervolgstap dan ook niet aan de orde.

Wij hebben vastgesteld dat op de volgende gebieden nog vervolgstappen nodig zijn om de bevindingen volledig weg te werken:

- Het aantoonbaar afhandelen van de lijst met de Belastingdienst applicaties die voorzien zijn van een bulk-export faciliteit;
  NB: Bovenstaande geldt ook voor de afhandeling van Belastingdienst applicaties waarbij nog geen schoningsfaciliteit aanwezig is;
- Het compleet maken en actualiseren van de verwerkersovereenkomsten in het AVG-register;
- Het ontwikkelen en implementeren van de kaders om tot meer uniforme inrichting van bedrijfsrollen te komen;
- Werkinstructies voor 'gebruik productiedata in test' nader uitwerken.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

Ten behoeve van dit onderzoek zijn de volgende werkzaamheden uitgevoerd.

Er zijn interviews gehouden met:
- De privacyofficer en de CISO van de Belastingdienst;
- De directeur en de datacoördinator van CAP;
- De datacoördinator van MKB;
- De datacoördinator van IV.

Bij gesprekken met MKB en IV was de desbetreffende directeur niet aanwezig. De directeur IV heeft akkoord gegeven op het gespreksverslag met de datacoördinator van IV.

Daarnaast is het AVG-register geanalyseerd en zijn diverse documenten opgevraagd en bestudeerd. De data-analyse door de ADR op de afname van de segmentvreemde rollen heeft niet integraal plaatsgevonden, omdat de aanwezige bronbestanden bij de ADR hiervoor niet geschikt waren. Daarentegen is er wel met een paar deelwaarnemingen in IMS de MKB rapportage over de afname van segmentvreemde rollen geverifieerd. Hiermee zijn de werkzaamheden overeenkomstig opdrachtbevestiging met kenmerk 2019-0000123351 uitgevoerd.

Object van onderzoek zijn:
- de aanbevelingen en bevindingen uit het ADR-onderzoek "Implementatie AVG bij het Ministerie van Financiën" met kenmerk 2019-0000062907, waarbij de peildatum van het onderzoek 28 februari 2019 was, met uitzondering van de bevindingen die gerelateerd zijn aan het verwijderen van oude persoonsgegevens;
- de brief van 28 mei 2019 van de staatssecretaris aan de Tweede Kamer waarin de Belastingdienst aangeeft op welke manier opvolging is gegeven aan de aanbevelingen van de ADR.

Als peildatum van het onderzoek is gehanteerd 1 september 2019.

Doelstelling van de aanvullende audit is om vast te stellen of de Belastingdienst de
- ADR-aanbevelingen heeft opgevolgd en of daarmee de eerder gerapporteerde bevindingen zijn opgelost, met uitzondering van de bevindingen die gerelateerd zijn aan het verwijderen van oude persoonsgegevens.

Deze doelstelling leidt tot de volgende onderzoeksvraag:
- Zijn de ADR-aanbevelingen ten aanzien van de door de Belastingdienst geformuleerde maatregelen zo opgepakt dat de onderliggende bevindingen als opgelost kunnen worden beschouwd?

Het onderzoek heeft alleen betrekking op de bevindingen die de ADR, bij het uitvoeren van het onderzoek naar de stand van zaken van een aantal maatregelen uit de implementatieplannen, heeft gedaan. Aan dit onderzoek kan dan ook geen conclusie worden ontleend aangaande het door de Belastingdienst al dan niet voldoen aan de AVG. Als in het kader van ons onderzoek relevante risico's met betrekking tot het voldoen aan de AVG naar voren komen, dan zullen wij deze rapporteren.

Ten aanzien van de ADR-bevindingen is geen separaat referentiekader gehanteerd, anders dan een algemene toets aan de AVG. Dit is conform het vorige onderzoek. NB: Er is geen inhoudelijke, juridische toets op de verwerkersovereenkomsten/verwerkersafspraken uitgevoerd.

De bevindingen zijn afgestemd middels hoor-wederhoor op 3 december 2019.

4.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd.

4.3 Verspreiding rapport

De opdrachtgever, de Directeur-Generaal Belastingdienst genaamd dr. J.J.M. Uijlenbroek, is eigenaar van dit rapport.

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

5 Ondertekening

Den Haag, 20 december 2019

auditmanager
Auditdienst Rijk

Managementreactie

De ADR heeft op mijn verzoek een aanvullend onderzoek uitgevoerd op de implementatie van de AVG bij de Belastingdienst. Dit aanvullende onderzoek is aangekondigd in de brief van de staatssecretaris aan de Tweede Kamer, d.d. 28 mei 2019.[8]

Ik dank de ADR voor het gedegen onderzoek dat is uitgevoerd.

De centrale boodschap van de ADR is dat de Belastingdienst met de aanbevelingen aan de slag is gegaan, maar dat er nog vervolgacties nodig zijn om alle bevindingen volledig op te lossen.

Op de genoemde vervolgacties geef ik hierbij mijn reactie.

Voldoen aan de AVG is een continu proces. Vervolgacties zullen er dan ook altijd zijn, immers de organisatie staat nooit stil.
De Belastingdienst is in het kader van de implementatie van de nieuwe organisatorische inrichting gestart met het beheersbaar toe kunnen kennen van autorisaties in de nieuwe organisatie. Het project "Rollenmodel 2.0" geeft daar invulling aan en draait op dit moment in pilot bij de directie Grote Ondernemingen. Overigens is het hebben van een segmentvreemde rol geen aanduiding voor een onterechte autorisatie.
Ik herken mij niet in de opmerkingen dat er geen voortgang zit op de registratie van verwerkingsovereenkomsten. Ten opzichte van de eerste audit ontbreekt één verwerkingsovereenkomst en de oorzaak daarvan is dat deze overeenkomst nog niet ondertekend is. Zodra de ondertekening rond is, wordt ook deze overeenkomst opgenomen in het register.
Ook hier geldt dat het register van verwerkingen geen statisch register is. Verwerkingen kunnen veranderen in de loop van de tijd, waarbij ik het belang onderschrijf dat het register van verwerkingen de actuele situatie weergeeft. De Functionaris Gegevensbescherming is voornemens om in 2020 opdracht te geven aan de ADR om een audit uit te voeren op het register van verwerkingen van het ministerie van Financiën. Daarbij wordt ook het deel van de Belastingdienst beoordeeld.
De opvolging van de inventarisatie van de bulk-exportfunctie is belegd bij de ketenvoorzitters van de betrokken informatiesystemen. Middels de architectuurlijn zou daar de sturing op plaats moeten vinden. Ik laat dat nader uitzoeken.
Ten slotte wordt er gewerkt aan de uitvoering van de werkinstructie "testen met productiedata" voor die gevallen waarbij het testen met gefabriceerde gegevens niet leidt tot het gewenste inzicht. Het niet hebben van een nieuwe werkinstructie wil overigens niet zeggen dat er daarom wel getest mag worden met productiedata. Ook voor de komst van de AVG was het testen met productiedata alleen toegestaan in bijzondere gevallen en na het treffen van adequate maatregelen. De nieuwe werkinstructie ziet dan ook grotendeels op de besluitvorming van het testproces. Die is met de nieuwe topstructuur wezenlijk anders.

8 Brief van 28 mei 2019 van de staatssecretaris aan de Tweede Kamer; Kamerstukken II 2018/19, 31 066, nr. 485

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00