Ministerie van Financiën

Rapport van bevindingen onderzoek gegevensgebruik D&A

periode van 1 februari 2016 tot 1 maart 2017

Versie 1.0

Datum 9 augustus 2017
Status Definitief

Colofon

Titel	Rapport van bevindingen onderzoek gegevensgebruik D&A
Auteurs	
Auditteam	
Bijlagen	N.v.t.
Inlichtingen	

Inhoud

1 Inleiding 6
1.1 Aanleiding 6
1.2 Context 6

2 Samenvatting 7

3 Doelstelling en verrichte werkzaamheden 8
3.1 Doelstelling 8
3.2 Verrichte werkzaamheden 8
3.3 Verspreidingskring rapportage 9

4 Bevindingen 10
4.1 Inrichting Data & Analytics (D&A) 10
4.2 Onderzoek naar de beveiliging bij D&A in de periode van 1 februari 2016 tot maart 2017 11
4.2.1 De Belastingdienst heeft het beveiligingsbeleid en de verantwoordelijkheden vastgelegd 11
4.2.2 Het beveiligingsbeleid van de Belastingdienst geeft een richtlijn voor monitoring, maar er is geen monitoring op het opmerken van datatransport door medewerkers van D&A. 11
4.2.3 Beveiligingsbeleid en -maatregelen D&A: op HBB aanvullende noodzakelijk geachte maatregelen niet volledig geïmplementeerd 11
4.2.3.1 Maatregelen organisatorische beveiliging: D&A hanteert maatregelen gericht op gedrag en faciliteiten van de medewerkers, maar nog niet volledig geëffectueerd . 11
4.2.3.2 Maatregelen fysieke beveiliging: er wordt voor D&A geen verbijzonderde toegangsbeveiliging toegepast 12
4.2.3.3 Maatregelen logische beveiliging: data op één centrale plek, maar logische scheiding niet mogelijk vanuit de beschikbare ICT service 12
4.3 Risico inventarisatie onderzoeksteam ter voorbereiding loggingsonderzoek 13
4.3.1 De analytische werkruimte biedt mogelijkheden om data over te brengen naar de werkplek en rechtstreeks naar buiten de Belastingdienst 13
4.3.2 De werkplek biedt mogelijkheden om data naar buiten de Belastingdienst te brengen 13
4.4 Onderzoek naar loggegevens om vast te stellen of getracht is gegevens buiten de Belastingdienst te brengen 13
4.4.1 Niet alle handelingen waarbij gegevens buiten de Belastingdienst kunnen worden gebracht zijn traceerbaar in de logging 13
4.4.2 Er zijn gegevens buiten de Belastingdienst gebracht 14
4.4.3 Er is datatransport zichtbaar zonder dat de inhoud vastgesteld kan worden 14
4.4.4 Er zijn gegevensopvragingen die niet aannemelijk lijken bij de functie van D&A 15

5 Ondertekening 16

1 Inleiding

1.1 Aanleiding

In het Kamerdebat d.d. 9 februari 2017 zijn vragen gesteld naar aanleiding van een tv uitzending van 1 februari 2017. In deze uitzending is gesteld dat bij het koppelen van gegevens voor fraudebestrijding door de Belastingdienst belangrijke beveiligingsrisico's aan het licht zijn gekomen. De Staatssecretaris van Financiën heeft naar aanleiding van het Kamerdebat meerdere onderzoeken toegezegd. Dit onderzoek naar het 'gegevensgebruik bij Data & Analytics (D&A)' is één van de in gang gezette beveiligingsonderzoeken.

1.2 Context

Het onderzoek gegevensgebruik D&A is onder opdrachtgeverschap van de DG Belastingdienst uitgevoerd door de Belastingdienst, onder direct gezag van de hoofddirecteur Informatievoorziening. De directeur Bedrijfsvoering IV is de opdrachtnemer. Het onderzoek is uitgevoerd door auditors van de IV-organisatie van de Belastingdienst. De onderzoekers zijn functioneel onafhankelijk van de afdeling D&A.

De objectiviteit en degelijkheid van het onderzoek is geborgd door een onderzoek van de aanpak en de uitvoering van het onderzoek en van de bevindingen door de Auditdienst Rijk (ADR). Dit is conform de toezegging in de brief van 14 februari 2017.

2 Samenvatting

Inleiding
De Staatssecretaris van Financiën heeft naar aanleiding van het Kamerdebat op 9 februari 2017 toegezegd onderzoek te zullen doen naar het 'gegevensgebruik bij Data & Analytics (D&A)'. Het onderzoek gegevensgebruik D&A heeft zich gericht op de periode 1 februari 2016 tot 1 maart 2017.

Beveiligingsmaatregelen D&A
Binnen de Belastingdienst is beveiliging als onderdeel van integraal management en bedrijfsvoering een verantwoordelijkheid van het lijnmanagement op de diverse niveaus van de organisatie met het Rijksbrede uitgangspunt het vertrouwen in de medewerker.
Het beveiligingsbeleid van de Belastingdienst geeft een richtlijn voor monitoring. Er wordt echter geen monitoring uitgevoerd op het detecteren van pogingen, door medewerkers van D&A, om data buiten de Belastingdienst te brengen.

D&A volgt het principe, dat in het beveiligingsbeleid van de Belastingdienst wordt gehanteerd, dat beveiliging werkt vanuit het eigen beveiligingsbewustzijn van de medewerker. D&A heeft in de onderzoeksperiode specifieke maatregelen ingezet om het beveiligingsbewustzijn van de (inhuur)medewerkers te bevorderen. Deze zijn deels geëffectueerd.
De door D&A gehanteerde analyseomgeving biedt geen projectgebonden autorisatie-structuur. Dit betekent dat projectmedewerkers toegang hebben tot alle data die binnen die omgeving zijn opgeslagen.

Buiten de Belastingdienst brengen van gegevens
Uit het onderzoek is gebleken dat het mogelijk is om gegevens buiten de Belasting-dienst te brengen. Wij hebben vastgesteld aan de hand van kritische deelwaar-nemingen op basis van de beschikbare loggegevens dat er in tien gevallen van deze mogelijkheid daadwerkelijk gebruik is gemaakt.

Oneigenlijk gegevensgebruik
Uit het onderzoek aan de hand van kritische deelwaarnemingen is niet uit te sluiten dat oneigenlijk gebruik van gegevens heeft plaatsgevonden.

3 Doelstelling en verrichte werkzaamheden

3.1 Doelstelling

De Staatssecretaris van Financiën heeft in zijn brief van 14 februari 2017 een nadere beschrijving gegeven van de onderzoeken die in zijn brief van 8 februari 2017 over de uitzending van Zembla, waren aangekondigd[1].
Het doel van het onderzoek naar D&A is als volgt omschreven.
"Doel van dit onderzoek is om aan de hand van in elk geval beschikbare loggegevens over gebruik van systemen, applicaties en data bij D&A vanaf de oprichting op 1 februari 2016 tot heden, vast te stellen of getracht is daadwerkelijk gegevens van belastingplichtigen, belastingschuldigen of toeslaggerechtigden buiten de Belastingdienst te brengen."

Op grond van deze doelstelling valt het onderzoek uiteen in twee delen:
- onderzoek naar opzet en bestaan van beveiligingsmaatregelen bij D&A om dit tegen te gaan;
- onderzoek naar de vraag of in de genoemde periode gegevens[2] buiten de Belastingdienst zijn gebracht.

3.2 Verrichte werkzaamheden

Deze opdracht is uitgevoerd overeenkomstig NOREA Richtlijn 4401, "Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie." In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd. Indien andere (aanvullende) werkzaamheden of een assurance-opdracht zouden zijn uitgevoerd, zouden wellicht andere onderwerpen zijn geconstateerd en gerapporteerd.

Dit rapport bevat feitelijke bevindingen van het onderzoeksteam over de periode van 1 februari 2016 tot 1 maart 2017. Er wordt geen samenvattend oordeel of conclusie gegeven over de mate van voldoen aan de van toepassing zijnde beveiligingsnormen, zoals onderdelen van het Handboek Beveiliging Belastingdienst (HBB).

Het onderzoeksteam heeft de te verrichten werkzaamheden samen met de opdrachtnemer, de directeur Bedrijfsvoering IV, afgestemd met de gedelegeerd/operationeel opdrachtgever, de hoofddirecteur IV.

Het onderzoek heeft zich gericht op:
- de beveiliging D&A in de periode van 1 februari 2016 tot 1 maart 2017;
- de loggegevens om vast te stellen of getracht is om gegevens van burgers en bedrijven buiten de Belastingdienst te brengen in de periode van 1 februari 2016 tot 1 maart 2017.

Vanuit de infrastructuur en applicaties is op basis van een risicoanalyse geïnventariseerd welke scenario's voor het naar buiten brengen van gegevens

1 Kamerstukken II 2016/17, 31 066, nrs. 340 en 344.
2 Met gegevens wordt bedoeld: gegevens van belastingplichtigen, belastingschuldigen of toeslaggerechtigden.

mogelijk zijn. Vervolgens is nagegaan hoe dit naar buiten brengen van gegevens via beschikbare logdata traceerbaar zou zijn. Middels tooling zijn uit de beschikbare logging handelingen geselecteerd die mogelijk duiden op het naar buiten brengen van gegevens en/of oneigenlijk gegevensgebruik[3]. Hierop zijn (kritische) deelwaarnemingen gedaan.

De aard van de materie/het onderzoeksobject brengt inherente beperkingen met zich mee. Het is niet mogelijk om alle al dan niet geslaagde pogingen om gegevens buiten de Belastingdienst te brengen vast te stellen.
Dit is bijvoorbeeld te wijten aan situaties die niet te loggen zijn. Bij het laatste kan gedacht worden aan het meenemen van printjes met gegevens en fotografische vastleggingen van gegevens.

Over de wijze van uitvoering van de opdracht is frequent overleg geweest met de opdrachtgever. Zo is in aanvulling op de opdracht onderzoek gedaan naar het oneigenlijk gebruik van gegevens en zijn bevindingen hierover in deze rapportage opgenomen.

De vanuit de doelstelling van dit onderzoek relevante bevindingen zijn weergegeven in dit rapport. Bevindingen met een vertrouwelijk karakter zijn niet in detail opgenomen.

3.3 Verspreidingskring rapportage

De directeur Bedrijfsvoering IV verstrekt deze rapportage aan de opdrachtgever, de DG Belastingdienst, en de gedelegeerd/operationeel opdrachtgever, de hoofddirecteur IV.

3 Gegevensopvragingen die niet aannemelijk lijken bij de functie van D&A

4 Bevindingen

4.1 Inrichting Data & Analytics (D&A)

Totstandkoming D&A
Het dienstonderdeel D&A is op 1 februari 2016 opgericht. De verkennende fase startte al in 2012, in het programma "Broedkamer". Bij D&A werken interne en externe specialisten samen op de terreinen als datascience, -operatie en -beheer. Hun taak is de gegevens (ook: data) in de transactiesystemen (ook: bronsystemen) van de Belastingdienst toegankelijker en beter bruikbaar te maken. Zo dragen zij bij aan een nieuwe, informatiegestuurde manier van werken van de Belastingdienst.

Verschillende onderzoeken/adviesopdrachten hebben gekeken naar organisatie-inrichting en (beveiliging van) datagebruik bij (voorgangers) D&A (Oliver Wyman 2015, LiquidHub 2015, ADR 2016[4]). Wij hebben geen formele besluitvorming ten aanzien van deze rapporten aangetroffen.

Werkwijze D&A
D&A maakt innovatieve informatietoepassingen voor toezichtmedewerkers en medewerkers in de administratieve processen (t.b.v. informatiegestuurde handhaving en/of inning), en voor bestuurders en managers (t.b.v. sturing, verantwoording en effectmeting).

Binnen de Belastingdienst voorhanden data zijn de grondstof van D&A-producten. De ruwe brondata worden benut om datafundamenten te bouwen door de data systematisch te ordenen en te bewerken en op te werken tot informatie die eenduidig te interpreteren en gemakkelijk te presenteren is voor verschillende doeleinden.
De technische inrichting van de dataopslag is gebaseerd op het principe van één centrale datavoorziening als basis voor de datafundamenten.

De datafundamenten leveren inzichten over bestaande informatieposities heen. Dat kan zijn over de dienstonderdelen heen, over belastingmiddelen heen, per proces-keten of per (groep) belastingplichtige(n) of toeslaggerechtigden.
De inzichten vormen de basis voor te maken keuzes in het uitvoeren van toezicht en inning/invordering.

IT ondersteuning D&A
D&A maakt voor het realiseren van datafundamenten en het leveren van informatieproducten gebruik van een analytische werkruimte (een ICT-service bestaande uit hard- en software), AWS+ geheten. D&A heeft vier AWS+ omgevingen in gebruik. In deze werkruimtes wordt gewerkt met een kopie van gegevens uit de bronsystemen van de Belastingdienst.
De AWS+ wordt door het Belastingdienstonderdeel IV-accent geleverd sinds 2014.

Het werken met een AWS+ vereist een werkplek, daarvoor wordt de Digitale Werkplek Belastingdienst (DWB) gebruikt. De DWB biedt digitale technologie aan

4 'Review of Investeringsagenda De Belastingdienst', 20 mei 2015 (Oliver Wyman); 'Belastingdienst BIA Observaties & Aanbevelingen', 26 maart 2015 (LiquidHub); 'Investigating Data Streams', december 2015 (Oliver Wyman); 'Onderzoek borgingsmaatregelen D&A', 10 maart 2016 (ADR)

eindgebruikers, waarmee zij in staat worden gesteld om hun dagelijks werk te verrichten, zowel vanaf pc- werkplekken als mobiele devices.

4.2 Onderzoek naar de beveiliging bij D&A in de periode van 1 februari 2016 tot maart 2017

4.2.1 De Belastingdienst heeft het beveiligingsbeleid en de verantwoordelijkheden vastgelegd

Binnen de Belastingdienst is beveiliging als onderdeel van integraal management en bedrijfsvoering een verantwoordelijkheid van het lijnmanagement op de diverse niveaus van de organisatie met als Rijksbrede uitgangspunt het vertrouwen in de medewerker. Het beveiligingsbeleid en de beveiligingsnormen van de Belastingdienst zijn vastgelegd in het Handboek Beveiliging Belastingdienst (HBB).

Het HBB betreft het basis-beveiligingsniveau; uitwerkingen van het HBB en noodzakelijk geachte aanvullende maatregelen worden binnen de dienstonderdelen bepaald op basis van een risico- en/of kwetsbaarhedenanalyse.

4.2.2 Het beveiligingsbeleid van de Belastingdienst geeft een richtlijn voor monitoring, maar er is geen monitoring op het opmerken van datatransport door medewerkers van D&A.

In het HBB, hoofdstuk 'Beveiliging bedrijfsvoering', is een richtlijn voor het monitoren van activiteiten opgenomen.

Er is geen monitoring op het detecteren van pogingen, door medewerkers van D&A, om data buiten de Belastingdienst te brengen.

4.2.3 Beveiligingsbeleid en -maatregelen D&A: op HBB aanvullende noodzakelijk geachte maatregelen niet volledig geïmplementeerd

D&A maakt gebruik van de binnen de afdeling BI&A (voorloper van D&A) op 7 december 2015 uitgevoerde 'bedreigingen- en kwetsbaarhedenanalyse'. Dit heeft geresulteerd in het benoemen van een aantal noodzakelijk geachte aanvullende maatregelen. Deze zijn nog niet allemaal binnen de onderzoeksperiode geïmplementeerd en worden hierna op hoofdlijnen toegelicht.

4.2.3.1 Maatregelen organisatorische beveiliging: D&A hanteert maatregelen gericht op gedrag en faciliteiten van de medewerkers, maar nog niet volledig geëffectueerd

Met ingang van mei 2016 is de functie van Data Protectie Functionaris geformaliseerd binnen D&A. De in deze functie benoemde medewerker was vanaf oktober 2014 binnen de afdeling BI&A werkzaam op het gebied van bescherming van gegevens.

Tot begin 2017 hadden vijf interne medewerkers binnen D&A een USB-ontheffing voor activiteiten rondom dataleveringen. Op 10 januari 2017 is besloten om alle USB-ontheffingen in te trekken; per 26 januari 2017 zijn deze ontheffingen ingetrokken. Op 9 februari bleek dat nog één persoon, die administratief onder een ander organisatieonderdeel viel, over een USB-ontheffing beschikte. Deze ontheffing is na constatering direct ingetrokken.

In mei 2015 werd een bewustwordingsprogramma verplicht gesteld voor alle medewerkers van BI&A en later D&A. Dit programma bestond uit plenaire trainingen Privacy en Security en een cursus iBewustzijn Overheid. Eind februari 2017 zijn 151 van de 172 medewerkers D&A (zowel intern als extern) naar de plenaire Privacy en Security training geweest en hebben 73 medewerkers de cursus iBewustzijn Overheid gedaan.

4.2.3.2 Maatregelen fysieke beveiliging: er wordt voor D&A geen verbijzonderde toegangsbeveiliging toegepast

D&A maakt gebruik van de standaard-dienstverlening voor toegangsbeveiliging van Belastingdienstgebouwen, verleend door de Centrale Facilitaire Dienst (CFD) van de Belastingdienst. De hoofdingang en personeelsingang van het gebouw waarin D&A gehuisvest is, zijn voorzien van tourniquets met kaartlezers. Ook zijn de afzonderlijke etages voorzien van kaartlezers; de toegangsdeuren kunnen met een Rijkspas geopend worden door medewerkers van de Belastingdienst die niet bij D&A werkzaam zijn.

4.2.3.3 Maatregelen logische beveiliging: data op één centrale plek, maar logische scheiding niet mogelijk vanuit de beschikbare ICT service

De data-analyseomgeving biedt geen scheiding van omgevingen
De AWS+ kent geen logische scheiding van test-, pilot en productieomgevingen. Dit betekent dat wijzigingen gevolgen kunnen hebben voor de beschikbaarheid en betrouwbaarheid van informatieproducten t.b.v. informatiegestuurde handhaving en/of inning.

De data-analyseomgeving biedt geen projectgebonden autorisatiestructuur
Inzet van de AWS+ voor meerdere projecten, brengt een risico op oneigenlijk gebruik van gegevens met zich mee.
De AWS+ kent een op rollen gebaseerde autorisatiestructuur, echter binnen één AWS+ zijn deze rollen generiek en dus niet te differentiëren voor projecten. Bij D&A worden meerdere projecten binnen één AWS+ uitgevoerd. De projectmedewerkers hebben daardoor toegang tot alle data die op de desbetreffende AWS+ zijn opgeslagen. Als een medewerker bijvoorbeeld alleen betrokken is bij OB-projecten dan kunnen gegevens uit andere bronsystemen niet voor deze medewerker worden afgeschermd.

4.3 Risico inventarisatie onderzoeksteam ter voorbereiding loggingsonderzoek

Het onderzoeksteam heeft na de analyse van het systeemlandschap van D&A en het beveiligingsbeleid de specifieke risico's in beeld gebracht bij de toegang en het gebruik van gegevens.

4.3.1 De analytische werkruimte biedt mogelijkheden om data over te brengen naar de werkplek en rechtstreeks naar buiten de Belastingdienst

De software, gebruikt in de AWS+, maakt het mogelijk om gegevens waarmee gewerkt wordt op te slaan op de DWB, maar óók deze te mailen rechtstreeks vanuit de AWS+ (zonder tussenkomst van de DWB met de daarop geïnstalleerde e-mail functionaliteit). Dit brengt een risico met zich mee op het naar buiten brengen van gegevens (zie ook 4.4.3).

4.3.2 De werkplek biedt mogelijkheden om data naar buiten de Belastingdienst te brengen

In het ontwerp van de DWB is een balans gezocht tussen beveiligingsmaatregelen en de eigen verantwoordelijkheid en het bewustzijn van de gebruiker.

De gebruikte DWB is beveiligd, maar de hierop aangeboden functionaliteit biedt mogelijkheden om data buiten de Belastingdienst te brengen. Zoals bijvoorbeeld de mogelijkheid om e-mail met bijlagen te versturen.

4.4 Onderzoek naar loggegevens om vast te stellen of getracht is gegevens buiten de Belastingdienst te brengen

Deze paragraaf behandelt de uitkomsten van het loggingsonderzoek naar het buiten de Belastingdienst brengen van gegevens.

4.4.1 Niet alle handelingen waarbij gegevens buiten de Belastingdienst kunnen worden gebracht zijn traceerbaar in de logging

Er zijn handelingen mogelijk waarbij gegevens buiten de Belastingdienst kunnen worden gebracht die technisch niet te loggen zijn (bijvoorbeeld: het meenemen van printjes met gegevens en fotografische vastleggingen van gegevens).

Bij USB-sticks wordt het gebruik gelogd, van e-mail wordt de verzending gelogd, maar de inhoud van het dataverkeer in beide gevallen niet.

De bewaartermijn van gegevens, die nodig zijn om vast te stellen wat er is getransporteerd, is soms beperkt. Om vast te stellen wat er is gebeurd dienen loggegevens te worden gecombineerd met gegevens uit andere bronnen. Om bijvoorbeeld te kunnen achterhalen wat de inhoud van een e-mail is, inclusief eventuele bijlagen, dient gebruik te worden gemaakt van (backups van) het e-mailsysteem. Dit is alleen mogelijk als de e-mailbox inclusief de betreffende e-mail hierin nog beschikbaar is. Dit betekent dat verwijderde e-mails niet meer te achterhalen zijn.

4.4.2 Er zijn gegevens buiten de Belastingdienst gebracht

Het onderzoek middels een kritische deelwaarneming heeft aangetoond dat in de volgende gevallen gegevens buiten de beveiligde omgeving van de Belastingdienst zijn gebracht.

- In december 2016 is een e-mail met bijlage verzonden met daarin van 250 belastingplichtigen informatie over onder andere inkomen, inkomen partner, belastingschuld en banktegoed. Deze e-mail is gestuurd naar een e-mailaccount van een bedrijf.
- In december 2016 zijn drie e-mails verstuurd met in de 'onderwerpregel' een fiscaal nummer. Per e-mail is één risicopost uit het project 'aangifte OB' opgenomen met naam en nummer van de onderneming. De bijlage bevat informatie over aangiften Omzetbelasting.
- In november 2016 is een e-mail verstuurd met een bijlage. De inhoud ervan betreft de adresgegevens van twee fiscale nummers.
- In oktober 2016 is een e-mail verstuurd met gegevens uit een Inkomstenbelastingaangifte van één belastingplichtige.
- In augustus 2016 heeft een inhuurmedewerker een e-mail met gegevens in de bijlage verstuurd vanaf zijn werkgevers-account naar e-mailaccounts van de Belastingdienst. De bijlage bevat 83.220 fiscale nummers (bevat geen NAW-gegevens) met een advies over de voorgestelde behandeling door inning. Vastgesteld is dat deze gegevens op een eerder moment vanuit de analyseomgeving (AWS+) naar dat werkgevers-account zijn verstuurd.
- In juli 2016 is een e-mail verstuurd met een bijlage met gegevens Inkomstenbelasting 2011 van 50.000 belastingplichtigen (groep grensarbeiders).
- In juli 2016 is dezelfde e-mail met een bijlage met gegevens Inkomstenbelasting 2011 van 50.000 belastingplichtigen (groep grensarbeiders) nog een keer verzonden.
- In mei 2016 is een e-mail verstuurd met twee behandelopdrachten met fiscale gegevens van een belastingplichtige.
- In mei 2016 is een e-mail verstuurd met één behandelopdracht met fiscale gegevens van een belastingplichtige.
- In mei 2016 is een e-mail verstuurd met een bestand met 3.568 fiscale nummers (bevat geen NAW-gegevens) die in relatie worden gebracht met de 'Panamapapers'.

4.4.3 Er is datatransport zichtbaar zonder dat de inhoud vastgesteld kan worden

Tijdens het onderzoek zijn gevallen geconstateerd waarbij datatransport zichtbaar is, maar de inhoud niet (meer) vastgesteld kon worden binnen de Belastingdienst-omgeving. Er is bijvoorbeeld data getransporteerd middels webmail en er is data verplaatst naar een Amazon server.

Daarnaast zijn e-mails aangetroffen die opvallen door naamgeving van de bijlage en/of de 'onderwerpregel'.

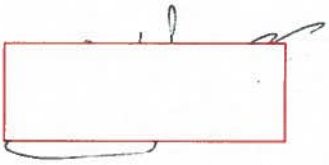
4.4.4 Er zijn gegevensopvragingen die niet aannemelijk lijken bij de functie van D&A

Bij D&A wordt gezocht naar structuren en verbanden in data. Daarbij is het niet aannemelijk dat gerichte gegevensopvragingen naar individuele belastingplichtigen/ toeslaggerechtigden worden gedaan.
Uit het onderzoek blijkt dat wel individuele gegevensopvragingen zijn gedaan, waardoor oneigenlijk gebruik van gegevens niet valt uit te sluiten. Voorbeelden zijn zoekacties naar bankrekeningnummers van individuen en naar individuele fiscale nummers.
Daarnaast heeft mogelijk oneigenlijk gebruik van gegevens plaatsgevonden door een geconstateerde opvraging van gegevens over VIP's[5].

5 Belastingplichtigen die een hoge openbare functie vervullen of die om één of andere reden in publicitaire zin een kwetsbare positie bekleden.

5 Ondertekening

Ondergetekende verklaart dat dit onderzoek overeenkomstig de daarbij gestelde zorgvuldigheidseisen is uitgevoerd.

[redacted] *(aspirant RE)*	[redacted] *RE MBA*
(Auditor IV-organisatie Belastingdienst)	*(Auditor IV-organisatie Belastingdienst)*
	
9 augustus 2017	*9 augustus 2017*