Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport ADR inzake het onderzoek van de Belastingdienst naar gegevensgebruik D&A

definitief

Colofon

Titel	Onderzoeksrapport ADR inzake het onderzoek van de Belastingdienst naar gegevensgebruik D&A
Uitgebracht aan	Secretaris-Generaal Financiën mw. M.R. Leijten
Datum	22 augustus 2017
Kenmerk	2017-0000140445

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Naar aanleiding van een TV-uitzending over de informatiebeveiliging bij het onderdeel Data & Analytics van de Belastingdienst, heeft de Staatssecretaris van Financiën aan de Tweede Kamer een aantal door de Belastingdienst uit te voeren onderzoeken en acties toegezegd. Voor een tweetal van deze onderzoeken en één actie is aan de ADR opdracht gegeven om hier onderzoek naar uit te voeren. De onderzoeken en actie van Belastingdienst betreffen:

1. Onderzoek gegevensgebruik bij D&A;
2. Onderzoek naar informatiebeveiliging bij de Broedkamer en voorlopers;
3. Actie naar de wijze waarop de eisen uit het Handboek Beveiliging Belastingdienst zijn geïmplementeerd in de organisatie, processen en systemen.

De ADR wordt betrokken om de objectiviteit en degelijkheid in de aanpak, de uitvoering en de rapportage van bevindingen te borgen.

Dit rapport is de uitwerking van het onderzoek door de ADR naar het onderzoek gegevensgebruik bij D&A door de Belastingdienst.

Samenvatting beantwoording onderzoeksvragen

De Belastingdienst heeft naar aanleiding van signalen over de beveiligingssituatie bij de eenheid D&A, een aantal onderzoeken in gang gezet om nader inzicht te verkrijgen. Ter borging van de objectiviteit en de degelijkheid van de door de Belastingdienst uit te voeren onderzoeken, heeft de Belastingdienst hiertoe een aantal maatregelen getroffen. In dat kader is ADR gevraagd onderzoek te doen naar de objectiviteit en degelijkheid van de door Belastingdienst uitgevoerde onderzoeken. De naar aanleiding van ons onderzoek samengevatte antwoorden op de 2 onderzoeksvragen bij het onderzoek van de Belastingdienst "Onderzoek gegevensgebruik D&A periode 1 februari 2016 tot en met 1 maart 2017", zijn:

Is de objectiviteit van de door de Belastingdienst uit te voeren onderzoeken D&A en Broedkamer en actie HBB geborgd?

- De aansturing en uitvoering van het onderzoek is geschied door medewerkers die functioneel onafhankelijk zijn van het organisatie onderdeel D&A;

Is de degelijkheid van de door de Belastingdienst uit te voeren onderzoeken D&A en Broedkamer en actie HBB geborgd?

- Het door de Belastingdienst uitgevoerde onderzoek en de opgestelde rapportage is uitgevoerd onder toepassing van de algemene kwaliteitseisen van de beroepsorganisatie NOREA en de specifieke eisen van de NOREA-richtlijn 4401.

Onze bevindingen bij de door de Belastingdienst getroffen maatregelen zijn in hoofdstukken 1 en 2 van dit rapport uitgewerkt.

1 Borging objectiviteit van uitvoering van het onderzoek gegevensgebruik D&A

1.1 Uitvoering van het onderzoek door medewerkers Belastingdienst die functioneel onafhankelijk zijn van D&A

Het onderzoek gegevensgebruik D&A is in opdracht van de DG Belastingdienst uitgevoerd door Belastingdienstmedewerkers, onder verantwoordelijkheid van de hoofddirecteur Informatievoorziening. De in het onderzoek betrokken afdeling D&A viel in de onderzoeksperiode niet onder de verantwoordelijkheid van de hoofddirecteur Informatievoorziening, maar werd aangestuurd door de Chief Financial Officer (CFO) Belastingdienst.
De directeur Bedrijfsvoering IV is de opdrachtnemer van het onderzoek.
Het onderzoek is uitgevoerd door auditors van de IV-organisatie van de Belastingdienst, aangevuld met een tweetal ingeleende medewerkers van andere onderdelen van de Belastingdienst (niet van D&A). Vastgesteld is dat alle onderzoekers functioneel onafhankelijk zijn van de afdeling D&A.

1.2 Deskundigheid medewerkers onderzoeksteam

Het onderzoeksteam bestaat uit 8 medewerkers. Hiervan zijn 3 medewerkers ingeschreven in het NOREA-register1 en hebben 2 medewerkers de post-doctorale EDP-auditopleiding afgerond.

1 NOREA is de beroepsorganisatie van IT-auditors in Nederland

2 Borging van de degelijkheid van het onderzoek gegevensgebruik D&A

2.1 Uitwerking opdracht volgens NOREA-richtlijn 4401

Het vertrekpunt voor de opdracht is de toezegging door de Staatssecretaris aan de 2e Kamer. Binnen de Belastingdienst is een opdrachtgever en opdrachtnemer benoemd en is een onderzoeksteam samengesteld, met inachtneming van eisen op het gebied van onafhankelijkheid en deskundigheid (zie hiervoor hoofdstuk 1).

Gekozen is om de opdracht uit te voeren volgens de NOREA-richtlijn 4401. Dit betreft een opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatie-technologie.

De NOREA-richtlijn 4401 is een passende richtlijn voor het onderhavige type onderzoek. In de NOREA 4401-richtlijn is oa. opgenomen dat de EDP-auditor uitsluitend verslag doet van de uitgevoerde werkzaamheden en de feitelijke bevindingen en geeft hij geen conclusie. De gebruikers van het rapport dienen zich zelf een oordeel te vormen betreffende de werkzaamheden en bevindingen die door de EDP-auditor in het rapport zijn weergegeven en hun eigen conclusies te trekken uit de door de EDP-auditor verrichte werkzaamheden.

2.2 Doel van de opdracht, het object van onderzoek en periode van uitvoering

Het doel van de opdracht is beschreven in het plan van aanpak:
"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."

Het object van onderzoek is:

- 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.

De uitvoering van het onderzoek heeft plaatsgevonden in de periode maart 2017 t/m juli 2017.

2.3 Plan van aanpak

De opdracht is door het onderzoeksteam van de Belastingdienst uitgewerkt in een plan van aanpak. Dit plan van aanpak "Onderzoek gegevensgebruik D&A" van 13 april 2017, is op 14 april ondertekend door de opdrachtnemer en op 19 april door de gedelegeerd opdrachtgever. In het plan van aanpak is de volgende inhoudsopgave opgenomen:

Inhoud

In het plan van aanpak zijn de volgende onderwerpen uitgewerkt:

- doel van de opdracht (situatie, probleem, wensen);
- afbakening en reikwijdte (wat wordt wel en niet meegenomen in de opdracht);
- kaders en uitgangspunten zoals bijvoorbeeld mate van diepgang, doorlooptijd en aannames;
- referentiekader;
- te hanteren standaard(en) vanuit NBA, NOREA en/of IIA (afhankelijk van de deskundigheid van de auditor c.q. de beroepsgroep waar de auditor is ingeschreven;
- te verwachten resultaten van de opdracht (op te leveren 'producten');
- plan van aanpak met werkzaamheden, mijlpalen en (tijds)fasering -> ;planning;
- inzet van mensen en middelen;
- rollen, taken en verantwoordelijkheden opdrachtgever en auditor;
- overleg en communicatie tijdens de opdracht;
- afronding en wijze van evaluatie met de opdrachtgever.

2.4 Werkprogramma

In bijlage 2 van het plan van aanpak Onderzoek gegevensgebruik D&A is het werkprogramma van het onderzoek gegevensgebruik D&A opgenomen. In het werkprogramma zijn de verschillende uit te voeren werkzaamheden verdeeld over de teamleden. Hierbij is rekening gehouden met de voor de uitvoering van de werkzaamheden benodigde kennis.
Van elk afgenomen interviews is een verslag opgesteld, welk is afgestemd met de geïnterviewde. De voor het onderzoek bestudeerde documenten zijn evenals de bij de uitvoering van het onderzoek naar de loggegevens gebruikte correspondentie, lijstwerk en opgevraagde documentatie opgenomen in het dossier. De in het werkprogramma opgenomen werkzaamheden zijn op 18 juli 2017afgerond, het dossier is afgesloten op dezelfde datum afgesloten.

2.5 Analyse

Bij de uitvoering van het onderzoek is gebruik gemaakt van een bevindingenmatrix. In de bevindingenmatrix is van elke onderzochte norm, de aangetroffen bevindingen, de bijbehorende bron en onderliggende document systematisch vastgelegd.
De aangetroffen bevindingen zijn in een overzicht opgenomen. Dit overzicht is ter afstemming voorgelegd aan het verantwoordelijk management.

2.6 Dossiervorming

Het onderzoek heeft binnen de Belastingdienst als werknaam :"Onderzoek gegevensgebruik D&A". Over de uitkomsten van het onderzoek is op18 juli 2017 het definitieve rapport:"*Rapport van bevindingen onderzoek gegevensgebruik D&A (periode van 1 februari 2016 tot 1 maart 2017)*" uitgebracht.
De archivering van het dossier vindt plaats op een hiervoor specifiek gereserveerde ruimte, waarbij de toegang tot en mogelijkheid voor uitvoeren van werkzaamheden is verstrekt aan een beperkt aantal belastingdienstmedewerkers die betrokken zijn bij de uitvoering van het onderzoek en aan een beperkt aantal ADR-medewerkers betrokken bij de uitvoering van het onderzoek van de ADR.

De door het onderzoeksteam gedane bevindingen zijn afgestemd en in het dossier te herleiden naar de bron.

De relevante documenten zijn aangetroffen in het dossier. De relatie tussen planning, uitvoering, analyse en rapportage is zichtbaar in verschillende documenten.

2.7 Afwegingsproces voor opname van bevindingen in de rapportage

De relatie tussen het bevindingenoverzicht en de rapportage (en de afweging daartussen) is opgenomen in: *"Wegingstabel bevindingen in rapportage".*
Het onderzoeksteam heeft in een afwegingsproces keuzes gemaakt wat betreft het opnemen van bevindingen in de rapportage. Zo zijn bevindingen met een vertrouwelijk karakter niet in detail in de rapportage opgenomen. In voorkomende gevallen is ervoor gekozen om bevindingen samenvattend op een hoger abstractieniveau weer te geven.

2.8 Rapportage

Het concept van dit rapport is besproken met de opdrachtgever.
Op 9 augustus 2017 is het definitieve rapport uitgebracht.
De volgende formeel vereiste onderwerpen zijn op juiste wijze opgenomen in de rapportage:

- een beschrijving van het doel en van de overeengekomen werkzaamheden;
- een opschrift dat duidelijk aangeeft dat dit een rapport van bevindingen betreft;
- de identificatie van de specifieke objecten waarop de overeengekomen specifieke werkzaamheden toegepast zijn;
- de vermelding dat de met de ontvanger overeengekomen werkzaamheden zijn uitgevoerd;
- de vermelding dat de opdracht is uitgevoerd overeenkomstig NOREA Richtlijn 4401: Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie;
- de beschrijving van het doel waarvoor de overeengekomen specifieke werkzaamheden zijn uitgevoerd;
- de beschrijving van de uitgevoerde specifieke werkzaamheden;
- de beschrijving van de feitelijke bevindingen van de IT-auditor, waaronder voldoende details van de gevonden fouten en afwijkingen;
- de vermelding dat geen assurance-opdracht is uitgevoerd en dat derhalve geen zekerheid over het object van onderzoek wordt verstrekt;
- de vermelding dat, indien de auditor andere aanvullende werkzaamheden of een assurance-opdracht zou hebben uitgevoerd, wellicht andere onderwerpen zouden zijn geconstateerd en gerapporteerd;
- eigenaarschap rapport;
- datum van het rapport;
- ondertekening.

In het rapport zijn feitelijke bevindingen opgenomen en wordt geen zekerheid verschaft en geen conclusie getrokken. In het rapport worden geen aanbevelingen gedaan. Dit is overeenkomstig de NOREA richtlijn 4401 en NOREA richtlijn 3000 voor Assurance-opdrachten.

3 Verantwoording onderzoek ADR

3.1 Werkzaamheden en afbakening

De ADR heeft overeenkomstig de opdrachtbevestiging onderzoek uitgevoerd naar het door de Belastingdienst uitgevoerde onderzoek gegevensgebruik D&A.
Onze werkzaamheden waren oa. het beantwoorden van de onderzoeksvragen aan de hand van het dossier van de Belastingdienst.
Het concept van dit rapport is afgestemd met de Belastingdienst en is op 18 juli 2017 besproken met de gedelegeerd opdrachtgever.

3.2 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.

3.3 Verspreiding rapport

De opdrachtgever, Secretaris-Generaal Financiën mevr. M.R. Leijten, 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.

4 Ondertekening

Den Haag, 22 augustus 2017

auditmanager
Auditdienst Rijk

Bijlage 1 Managementreactie

De Belastingdienst heeft naar aanleiding van signalen over de beveiligingssituatie bij de eenheid Data&Analytics, een aantal onderzoeken in gang gezet om nader inzicht te verkrijgen. De ADR is gevraagd om onderzoek te doen naar de objectiviteit en degelijkheid van de door Belastingdienst uitgevoerde onderzoeken. De antwoorden op de twee onderzoeksvragen van de ADR op het "Onderzoek gegevensgebruik D&A periode 1 februari 2016 tot en met 1 maart 2017", luiden dat:

- De aansturing en uitvoering van het onderzoek is geschied door medewerkers die functioneel onafhankelijk zijn van het organisatie onderdeel D&A;
- Het door de Belastingdienst uitgevoerde onderzoek en de opgestelde rapportage is uitgevoerd onder toepassing van de algemene kwaliteitseisen van de beroepsorganisatie NOREA en de specifieke eisen van de NOREA-richtlijn 4401.

Ik onderschrijf de beschreven aanpak, werkwijze en bevindingen en constateer dat de ADR geen nadere aanbevelingen doet. De Belastingdienst zal separaat een managementreactie verzorgen op het rapport gegevensgebruik D&A en daar vervolg aan geven.

Hoogachtend,

drs. M.R. Leijten
Secretaris-generaal Financiën

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