Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Aan Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA 's-Gravenhage

Directoraat-Generaal
Belastingdienst

Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Ons kenmerk
2017-0000192480

Uw brief (kenmerk)

Datum 2 oktober 2017
Betreft onderzoeken D&A, HBB en Broedkamer

Geachte voorzitter,

In februari 2017[1] heb ik uw Kamer geïnformeerd over verschillende onderzoeken en acties bij de Belastingdienst. Het betreft de volgende onderzoeken en acties:

1. Onderzoek uitgevoerd door de Autoriteit Persoonsgegevens.
2. Onderzoek gegevensgebruik bij Data & Analytics (verder: D&A), periode 1 februari 2016 tot en met 14 februari 2017.
3. Onderzoek naar informatiebeveiliging bij de Broedkamer en voorlopers, periode 2012 tot februari 2016.
4. Extern forensisch onderzoek naar de gevolgde aanbestedingsprocedure voor ondersteuning van de Broedkamer.
5. Overige acties:
    a. Bezien wordt op welke wijze het Handboek Beveiliging Belastingdienst (verder: HBB) is geïmplementeerd in de organisatie, processen en systemen.
    b. Medewerker(-tevredenheidsonderzoek) in het najaar 2017 bij Belastingdienst waarin onder andere vragen over werkcultuur en managementstijl meegenomen worden.

Met deze brief bied ik uw Kamer de rapporten aan van het onderzoek gegevensgebruik D&A[2], het onderzoek informatiebeveiliging Broedkamer[3] en onderzoek implementatie HBB[4]. Tevens bied ik de bij de rapporten behorende rapportages[5] van de Auditdienst Rijk (verder: ADR) aan. Het extern forensisch

[1] Kamerstuk 31 066, nr. 344, Kamerstuk 31 066, nr. 340
[2] Bijlage 1: Rapport van bevindingen onderzoek gegevensgebruik D&A, periode van 1 februari 2016 tot 1 maart 2017
[3] Bijlage 2: Rapport van bevindingen onderzoek informatiebeveiliging programma Broedkamer en voorlopers
[4] Bijlage 3: Onderzoek Implementatie HBB Eindrapport
[5] Bijlage 4: Rapporten ADR:
I. Onderzoeksrapport ADR inzake het onderzoek van de Belastingdienst naar gegevensgebruik D&A

onderzoek naar de aanbesteding D&A staat gepland om eind oktober te worden afgerond. Het medewerkerstevredenheidsonderzoek is eind dit jaar af. Voor het onderzoek van de Autoriteit Persoonsgegevens is nog geen opleverdatum bekend.

De voorlopige resultaten van het Onderzoek gegevensgebruik D&A waren aanleiding voor mij om uw Kamer op 30 juni[6] en 4 juli[7] jongstleden te informeren over tien aangetroffen gevallen van ongeoorloofd buiten de Belastingdienst brengen van persoonsgegevens. Ik heb destijds aanvullende acties en stappen aangekondigd. Met deze brief informeer ik uw Kamer over de resultaten van deze acties en stappen.

Geen indicaties van niet-functioneel gebruik
Mijn conclusie op basis van de bevindingen in de rapporten Onderzoek informatiebeveiliging Broedkamer en Onderzoek gegevensgebruik D&A, inclusief aanvullend leveranciersonderzoek is dat in een aantal casussen persoonsgegevens buiten de Belastingdienst zijn gebracht voor werkgerelateerde bewerking of analyse. Dat is tegen de regels en niet acceptabel. De belastingplichtige moet er vanzelfsprekend van kunnen uitgaan dat zijn persoonsgegevens binnen de systemen[8] van de Belastingdienst worden verwerkt en dat de regels hierbij worden nageleefd. Juist daarom verdient de bescherming van persoonsgegevens bij de Belastingdienst de hoogste aandacht en zorg. De binnen de Broedkamer en diens opvolger D&A, met medeweten van betrokken management gehanteerde werkwijze, voldeed niet aan deze norm.

Elk van de binnen het D&A- en Broedkameronderzoek gevonden casussen is nader onderzocht. Daarbij zijn geen indicaties gevonden dat persoonsgegevens niet-functioneel zijn gebruikt, anders gezegd de persoonsgegevens zijn voor werkdoeleinden gebruikt. Voor de D&A-casussen is door de leveranciers verklaard dat persoonsgegevens die buiten het bereik van de Belastingdienst zijn gebracht, inmiddels zijn vernietigd dan wel op een dusdanige wijze zijn zeker gesteld dat er niets meer mee kan gebeuren. Tevens is voor deze casussen op basis van onderzoek door betreffende leveranciers verklaard dat persoonsgegevens niet verder zijn verspreid.

De pilot Broedkamer groeide in de periode 2013 van 0 naar circa 130 medewerkers tot de huidige afdeling D&A om innovatieve technieken te ontwikkelen en te testen, zodat de Belastingdienst meer risicogericht en meer informatiegestuurd kan controleren en handhaven. De onzorgvuldigheid met betrekking tot persoonsgegevens binnen de Broedkamer en D&A wordt door twee factoren verklaard. Aan de ene kant kenden de bedrijfsonderdelen een te grote autonomie ten aanzien van de concrete invulling van de tactische HBB-kaders in de

II. Onderzoeksrapport ADR inzake het onderzoek van de Belastingdienst informatiebeveiliging programma Broedkamer en voorlopers.
III. Onderzoeksrapport ADR inzake de actie van de Belastingdienst implementatie HBB

[6] Kamerstuk 31 066, nr. 367
[7] Kamerstuk 31 066, nr. 369
[8] De Belastingdienst kent plaats- en tijdonafhankelijk werken waarbij gebruik van aan medewerkers van de Belastingdienst beschikbaar gestelde laptops op andere plaatsen dan een fysiek kantoor van de Belastingdienst geldt als werken binnen de Belastingdienstsystemen.

uitvoering. Aan de andere kant ontbrak op centraal niveau de regie op de goede invulling van het HBB bij de bedrijfsonderdelen van de Belastingdienst waardoor dit niet eerder werd gesignaleerd.

In de praktijk betekende dit dat er binnen de Broedkamer en D&A onvoldoende aandacht was voor het inrichten van monitoring van het conform beleid werken met persoonsgegevens zoals het HBB voorschrijft (van binnen naar buiten de Belastingdienst). Dit gegeven meldde ik uw Kamer al in mijn brief van 30 juni jongstleden. De monitoring was dominant gericht op bewaken van de continuïteit en monitoring van kwaadaardige invloeden van buiten naar binnen. Monitoring van uitgaand mailverkeer op persoonsgegevens vond niet systematisch plaats.

Vervolgacties sinds 30 juni 2017

In mijn brief van 30 juni jongstleden meldde ik u al aanvullende maatregelen en acties inzake D&A. Allereerst zijn de casussen gemeld bij de Autoriteit Persoonsgegevens en is er aangifte gedaan bij het Openbaar Ministerie. De relatie met bij de casussen betrokken externe medewerkers is per direct beëindigd. Betrokken interne medewerkers zijn onderworpen aan intern onderzoek dat inmiddels is afgerond. Gebleken is dat sprake was van een met medeweten van het management ontstane werkwijze. Het management en de medewerkers van D&A zijn over de onderzoeksbevindingen geïnformeerd en hen is duidelijk gemaakt tot welke wijziging in houding en gedrag dit moet leiden.

De beperking van de fysieke toegang tot de afdeling D&A is inmiddels gerealiseerd. Er is ook gewerkt aan verdere bewustwording op het gebied van werken met persoonsgegevens. Ook de toegang tot de analyse-omgevingen is direct na 30 juni jongstleden volledig afgesloten en individuele toegang wordt sindsdien op basis van een aangescherpte aanvraagprocedure verleend. Deze aangescherpte procedure blijft in ieder geval van toepassing tot de structurele oplossingen volledig geïmplementeerd zijn.

De binnen het D&A-onderzoek gevonden casussen zijn door de leveranciers onderzocht binnen hun eigen IT-omgeving. De leveranciers hebben bij de aangeleverde casussen en enkele door hen aanvullend aangetroffen casussen geen indicaties gevonden van niet-functioneel gebruik of verdere verspreiding van persoonsgegevens. De data van de casussen zijn vernietigd. Er is één casus waarbij een externe deskundige gebruik maakte van een private cloud-dienst voor tijdelijke opslag van de persoonsgegevens[9]. Er is vastgesteld dat ze niet meer aanwezig zijn.

Structurele oplossingen voor continue monitoring[10], pseudonimiseren[11] en datacompartimenteren[12] van de analyseomgeving D&A staan op stapel. De eerste

[9] Voor een cloud-dienst is, in tegenstelling tot de eigen technische infrastructuur van de leveranciers, niet te bepalen waar de data zich fysiek bevond.
[10] Monitoring is het vastleggen van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsprocedures registreren en behoren te worden bewaard en regelmatig te worden beoordeeld.
[11] Pseudonimiseren is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het gegeven is

actieve monitoring D&A wordt vierde kwartaal 2017 gerealiseerd. Implementatie van pseudonimisering/anonimisering is voorbereid. De start op de werkvloer staat gepland voor het eerste kwartaal 2018 met een doorlooptijd van een jaar. Compartimentering is volgens planning medio 2018 gerealiseerd. Totdat deze technische maatregelen zijn geïmplementeerd, blijven de procedurele maatregelen met aangescherpte ontheffingscriteria van kracht.

Naar aanleiding van de initiële melding van de casussen bij de Autoriteit Persoonsgegevens is door de Belastingdienst nader onderzoek verricht. Dit onderzoek wijst niet op negatieve gevolgen voor betrokken personen. Daarmee hoeven zij niet geïnformeerd te worden.

Het Openbaar Ministerie is geïnformeerd over de aanvullende onderzoeks-bevindingen na 30 juni. Het OM heeft recent het volgende laten weten:

"Uit het strafrechtelijk onderzoek blijkt dat in een aantal gevallen door extern ingehuurde medewerkers vertrouwelijke informatie uit de werkomgeving van de afdeling D&A naar eigen apparatuur buiten de belastingdienstorganisatie is gebracht. Als zodanig zou men zich in die gevallen niet gehouden hebben aan de door partijen ondertekende geheimhoudingsverklaringen.
Er is echter niet gebleken dat de informatie is gedeeld met personen buiten de groep personen werkzaam voor de afdeling D&A van de belastingdienst. Deze informatie is ook niet voor een ander doel gebruikt dan om verder te werken aan de voor en binnen de afdeling D&A gaande werkopdracht(en). Van enig opzettelijk handelen in het kader van Artikel 272[13] van het Wetboek van Strafrecht is niet gebleken. In verband hiermee is het onderzoek beëindigd."

Op basis van de uitkomsten van dit onderzoek en de aanvullende onderzoeken bij de leveranciers blijkt dat de wijze waarop met persoonsgegevens werd omgegaan bij de Broedkamer en D&A tekort schoot als gevolg van een te grote decentrale autonomie in combinatie met het tekort schieten van de centrale regie. Dit beeld ligt in het verlengde van eerdere waarnemingen over de informele werkwijze inzake besluitvorming en toezien op nakomen van kaderstellende afspraken[14] binnen de Belastingdienst.

Naar een bredere verankering van informatiebeveiliging binnen de Belastingdienst

Zoals eerder aangegeven zijn er geen indicaties gevonden van niet-functioneel gebruik. Desondanks til ik er zwaar aan dat de Belastingdienst niet altijd voldoende zorgvuldig met persoonsgegevens blijkt om te gaan en dat de top hier

---

daardoor niet op de «persoon herleidbaar» en daarmee geen persoonsgegeven in de zin van de Nederlandse Wet bescherming persoonsgegevens (Wbp).

[12] Compartimentering: De toegang tot in de data-analyseomgeving aanwezige gegevens is per medewerker beperkt tot alleen die gegevens die nodig zijn voor het specifieke werk dat men doet.

[13] Artikel 272 van het Wetboek van Strafrecht luidt, voor zover relevant : Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt (…) verplicht is het te bewaren, opzettelijk schendt, wordt gestraft (…).

[14] Bijlage bij Kamerstuk 31066 nr. 330 "Onderzoek naar de besluitvormingsprocedures binnen de Belastingdienst"

onvoldoende regie op heeft gevoerd. Dat moet anders – urgent – en dat is voor mij de belangrijkste conclusie naar aanleiding van de onderzoeken.

De informatiebeveiliging binnen de Belastingdienst moet worden verbeterd, zodat standaarden weer systematisch worden nageleefd. Informatiebeveiliging is, naast zaken als fiscale kwaliteit en operationele continuïteit, een kernwaarde van het management van de Belastingdienst. Dat moet gerichte en voortdurende aandacht geven aan de beveiliging van persoonsgegevens en daarop afrekenbaar zijn. De organisatorische inrichting wordt mede ingevuld door de implementatie van de nieuwe topstructuur voortkomend uit de aanbevelingen van de Commissie Onderzoek Belastingdienst[15].

Technische en organisatorische maatregelen alleen zijn niet voldoende. Iedere medewerker moet doordrongen zijn van het belang van informatiebeveiliging en de regels op dit terrein hebben geïnternaliseerd.

De direct na 30 juni jongstleden getroffen maatregelen waren al een krachtig signaal naar de medewerkers binnen de Belastingdienst en hebben het bewustzijn vergroot ten aanzien van persoonsgegevens. Daarmee is een eerste stap gezet. De Belastingdienst moet zich bewust zijn van de leidende positie die zij inneemt. Dit moet vertaald worden naar de zorgvuldigheid waarmee met persoonsgegevens wordt omgegaan. Ik zie dit als voorwaarde om het onwrikbare vertrouwen van burgers en bedrijven te blijven verdienen.

Via de Halfjaarrapportage Belastingdienst houd ik uw Kamer op de hoogte van de verdere ontwikkelingen.

Hoogachtend,

de staatssecretaris van Financiën,

Eric Wiebes

[15] 27 januari 2017