Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

31 066 Belastingdienst

Nr. 367 **BRIEF VAN DE STAATSSECRETARIS VAN FINANCIËN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 juni 2017

In het debat van 9 februari jl. heb ik met uw Kamer onder andere gesproken over databeveiliging bij de afdeling Data & Analytics (D&A) van de Belastingdienst. (Handelingen II 2016/17, nr. 51, items 5 en 8) Tijdens het debat heb ik onderzoek naar de databeveiliging bij de afdeling D&A aangekondigd. Hoewel dit onderzoek nog niet is afgerond, wil ik een aantal bevindingen en voorlopige conclusies alvast met uw Kamer delen.

In het onderzoek op basis van de logginggegevens zijn de onderzoekers gestuit op een aantal gevallen waarin persoonsgegevens op een ongeoorloofde manier de Belastingdienst hebben verlaten. Dat is niet acceptabel. De belastingbetaler moet ervan kunnen uitgaan dat zijn gegevens bij de Belastingdienst veilig zijn. Juist daarom verdient de bescherming van persoonsgegevens bij de Belastingdienst de hoogste aandacht en zorg. De voorlopige onderzoeksresultaten laten zien dat de afdeling D&A hierin tekort is geschoten. Deze voorlopige resultaten zijn voor mij aanleiding om direct maatregelen te nemen.

Hieronder ga ik achtereenvolgens in op de geconstateerde ongeoorloofde gegevensuitwisselingen, de genomen maatregelen en het vervolgtraject.

Voorlopige onderzoeksresultaten: ongeoorloofde gegevensuitwisseling

Het onderzoek naar de databeveiliging bij D&A betreft de periode februari 2016 – februari 2017. Basis voor het onderzoek zijn de loggingsgegevens van deze periode. Deze zijn geanalyseerd aan de hand van scenario's voor gevallen van ongeoorloofde gegevensuitwisseling. Op basis van deze risicogerichte onderzoeksaanpak zijn tien gevallen geconstateerd waar sprake is van een vorm van ongeoorloofde gegevensuitwisseling. Op dit moment bestaat daarvan het volgende beeld:

A. Eén geval betreft een gerichte selectie van personen met persoonlijke informatie over hen. Deze informatie is door externe medewerkers naar buiten gebracht via de e-mail. Dit geval kan nog op geen enkele

kst-31066-367
ISSN 0921 - 7371
's-Gravenhage 2017

wijze worden verklaard vanuit het werk dat bij D&A gebeurt. Op basis van deze onderzoeksbevindingen is aangifte gedaan.

B. Vijf gevallen betreffen gegevens van één persoon die via e-mail naar buiten werden verstuurd. Het gaat hierbij om een schending van de geldende normen, te meer daar er geen duidelijke relatie lijkt met het werk op deze afdeling. Ten aanzien van betrokken medewerkers zal een integriteitsonderzoek worden gestart op basis waarvan disciplinaire maatregelen kunnen worden getroffen. Ten aanzien van externe medewerkers zal de uitlenende organisatie worden gevraagd een integriteitsonderzoek te starten.
C. Bij twee gevallen, waarvan één met dubbele verzending, is nog nadere informatie nodig om vast te stellen of onzorgvuldig handelen danwel een integriteitsonderzoek aan de orde zijn. Dit betreffen selecties die vooralsnog werkgerelateerd lijken te zijn. Het gaat bijvoorbeeld om het extern bewerken van een bestand om dat na bewerking terug te plaatsen. De gegevens zijn soms wel en soms niet tot personen herleidbaar. De uitkomsten van deze selecties zijn via e-mail naar buiten gestuurd wat niet had gemogen.
D. Twee gevallen vereisen nader onderzoek om vast te stellen om wat voor gegevens het gaat, wat er met de gegevens is gebeurd en of de handelingen passen binnen het werk van de afdeling.

Het Openbaar Ministerie oriënteert zich momenteel op de aangifte. Tevens is melding gedaan aan de Autoriteit Persoonsgegevens (AP) van deze gevallen. De AP oriënteert zich nog op een eventueel onderzoek. Op korte termijn zullen betrokken bedrijven en personen conform de vereisten uit de Wet Bescherming Persoonsgegevens worden geïnformeerd over dit informatielek. De inhuur van de betrokken externe medewerkers is per direct beëindigd. Tevens is met de uitlenende organisaties overleg gestart om te achterhalen wat met de oneigenlijk uitgewisselde gegevens is gebeurd. Verdere juridische consequenties worden bezien.

De voorlopige resultaten van het onderzoek hebben ook duidelijk gemaakt dat binnen de afdeling D&A geen invulling is gegeven aan een vorm van reguliere monitoring. De richtlijn voor informatiebeveiligingen (het Handboek Beveiliging Belastingdienst, HBB) schrijft dit wel voor. Dit betekent dat in de praktijk wordt afgeweken van het HBB, waardoor mijn uitspraak tijdens het debat op 9 februari dat sprake was van logging[1] en monitoring[2], gebaseerd blijkt te zijn op een papieren werkelijkheid. Dat betreur ik. Logging heeft wel plaatsgevonden, actieve monitoring niet.

Genomen maatregelen

Sinds het debat van 9 februari zijn diverse aanvullende maatregelen genomen om de databeveiliging te verbeteren. Het gaat daarbij om het inperken van de fysieke toegang, diverse bewustzijnscampagnes richting de medewerkers, en het werken aan structurele (technische) oplossing van continue monitoring, pseudonimiseren[3] en datacompatimenteren[4]

---

[1] Vastlegging van handelingen van personen en meldingen met betrekking tot de technische infrastructuur.
[2] Vastleggen van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsprocedures registreren, behoren te worden bewaard en regelmatig te worden beoordeeld.
[3] Pseudonimiseren is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het gegeven is daardoor niet op de «persoon herleidbaar» en daarmee geen persoonsgegeven in de zin van de Nederlandse Wet bescherming persoonsgegevens (Wbp).
[4] 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.

van de analyseomgeving. Deze structurele oplossingen kosten evenwel tijd, nog minimaal zes maanden voor volledige implementatie.

Zolang deze structurele maatregelen met betrekking tot deze specifieke data-analyseomgeving nog niet gereed zijn, zullen maatregelen worden genomen die de mogelijkheid tot datatransfer van deze specifieke dataomgeving naar buiten de Belastingdienst onmogelijk maken. Om dit te realiseren wordt het gedurende enkele dagen onmogelijk gemaakt om toegang te krijgen tot de data-analyseomgeving. Ik ben me er van bewust dat dit ingrijpend is voor de werksituatie van de gebruikers van de data-analyseomgeving, maar dit is de enige manier om op dit moment maximale zekerheid te creëren dat oneigenlijke gegevensuitwisseling vanuit de data-analyseomgeving is uitgesloten. Op de reguliere controles door de Belastingdienst heeft dit geen invloed.

Vervolgtraject

Het onderzoek naar de databeveiliging bij de afdeling D&A heeft gevallen van oneigenlijk gegevensgebruik aan het licht gebracht. Het onderzoek is echter nog niet afgerond. Daarnaast zijn nog andere onderzoeken gaande waarvan de voortgang op 20 april aan uw Kamer is gemeld in de 19e halfjaarsrapportage Belastingdienst.[5]

Ik streef naar een snelle afronding van de onderzoeken en zal uw Kamer daarover informeren. Deze onderzoeken hebben een breder bereik dan alleen de afdeling D&A. Naast de technische inrichting van systemen moet binnen de hele Belastingdienst een hoog besef zijn van zorgvuldig gegevensgebruik. De organisatorische randvoorwaarde worden daarvoor ingericht met een nieuwe directie Informatievoorziening en Databeheersing als onderdeel van de nieuwe topstructuur Belastingdienst. Datarisico's krijgen zo op topniveau aandacht.

De hiervoor genoemde getroffen en te treffen maatregelen zullen ertoe leiden dat de informatiebeveiliging wordt verbeterd. De bewustwording op het gebied van het gebruik van gegevens is daar een belangrijk onderdeel van.

De Staatssecretaris van Financiën,
E.D. Wiebes

[5] Bijlage bij Kamerstuk 31 066, nr. 355.