AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
Staatssecretaris van Financiën
De heer drs. M. Snel
Korte Voorhout 7
2500 EE DEN HAAG

Datum
14-10-2019

Ons kenmerk
z2017-00499

Contactpersoon

070 8888 500

Onderwerp
Onderzoek naar Datafundamenten & Analytics

Geachte heer Snel,

In februari 2017 is de Autoriteit Persoonsgegevens een eerste onderzoek gestart naar de informatiebeveiliging van de toenmalige afdeling Data & Analytics (D&A), tegenwoordig Datafundamenten & Analytics (DF&A), van de Belastingdienst. De AP heeft u op 3 juli 2018 per brief geïnformeerd over de resultaten van het onderzoek en over de daarbij geconstateerde overtredingen. Daarnaast heeft de AP aan de Belastingdienst verzocht informatie te verstrekken over de getroffen verbetermaatregelen. Deze informatie gaf aanleiding tot een vervolgonderzoek. De AP informeert u met deze brief over de resultaten van het vervolgonderzoek.

De AP concludeert dat de getroffen verbetermaatregelen bij DF&A ten behoeve van de geconstateerde beveiligingsrisico's deze risico's dusdanig verminderen dat de eerder door de AP geconstateerde overtredingen niet langer voortduren.

Eerste onderzoek

De AP heeft in haar eerste onderzoek betreffende drie beveiligingsaspecten geconstateerd dat deze niet in orde waren, te weten:

1) Het ontbreken van de logging van de drie activiteiten: i) export van data vanuit de brongegevens naar de werkplek van een medewerker, ii) het schrijven van data op een usb-stick en iii) het opslaan van bijlagen op mobile devices.

2) De controle op de logging. Voor een deel van de logging vond er in zijn geheel geen periodieke controle plaats, omdat deze logging niet was aangesloten op het systeem waar actieve monitoring plaatsvindt. Voor het e-mailverkeer van DF&A dat wel was aangesloten op dit systeem bestond er geen periodieke controle van data die via e-mail buiten de Belastingdienst werd gebracht.
3) Het verwijderen/intrekken van autorisaties van medewerkers of extern ingehuurde medewerkers na uitdiensttreding én het verlenen van te ruime toegangsrechten aan de D&A medewerkers waardoor deze toegang hadden tot data die niet noodzakelijk was om hun werk uit te voeren.

Op 19 september 2018 heeft de Belastingdienst informatie verstrekt aan de AP over de getroffen verbetermaatregelen. Ook heeft de staatssecretaris van Financiën[1] in dit kader reactie gegeven op vragen van de Tweede Kamer. Dit tezamen leidde bij de AP tot het vermoeden dat nog niet alle geconstateerde tekortkomingen in de beveiliging van DF&A opgelost waren. Naar aanleiding hiervan is de AP een vervolgonderzoek gestart.

In dit kader heeft de AP op 9 mei 2019 verklaringen afgenomen van medewerkers en in vervolg hierop aanvullende schriftelijke vragen gesteld.

Vervolgonderzoek

Tijdens het vervolgonderzoek heeft de AP onderzocht of de eerder geconstateerde overtredingen bij DF&A nog voortduurden.

Ad 1) Ontbreken van de logging

Om te beoordelen of de onder 1) vermelde ontbrekende activiteiten kunnen worden aangemerkt als relevante activiteiten die gelogd moeten worden, heeft de AP in haar eerste onderzoek het ontbreken van de logging van die activiteiten in samenhang beoordeeld. In haar eerste onderzoek constateerde de AP dat het ontbreken van de logging van de export van data vanuit de brongegevens in combinatie met het ontbreken van logging van het transporteren van data naar een externe gegevensdrager, zoals een usb stick of een mobile device, een risico opleverde voor de beveiliging van die data. Door handelingen op externe gegevensdragers/opslag niet te loggen kon data namelijk ongemerkt worden gekopieerd of geëxporteerd. Dit hield in dat nergens in de keten werd vastgelegd door wie, welke data mogelijk onrechtmatig buiten de Belastingdienst werd gebracht. Hierdoor was het ook niet mogelijk om via controle op de logging op te merken dat data via deze weg de Belastingdienst onrechtmatig verliet. Achteraf kon niet worden nagegaan welke data door wie naar buiten was gebracht.

i) Downloaden/exporteren naar eigen werkplek

[1] TK, 2018-2019, Aanhangsel (antwoord staatssecretaris van Financiën), 19 november 2018. Reactie staatssecretaris van Financiën op vragen vaste commissie voor Financiën, 7 februari 2019. TK 2018-2019, 32 761, nr. 136 (antwoorden staatssecretaris van Financiën).

Zoals de AP in haar brief van 3 juli 2018 heeft gecommuniceerd, is uit het eerste onderzoek van de AP gebleken dat het downloaden en exporteren van bestanden naar de eigen werkplek/werkstation niet (standaard) werd gelogd.

Uit het vervolgonderzoek blijkt dat export van data vanuit de brongegevens naar het geheugen van de fysieke werkplek van een medewerker van DF&A nog steeds niet wordt gelogd. Echter, uit het onderzoek blijkt ook dat medewerkers deze exporthandeling niet vaak nodig hebben, omdat de meeste werkzaamheden binnen de analytische omgeving uitgevoerd kunnen worden. Daarnaast dienen medewerkers hiervoor nu ook toestemming te vragen aan de betreffende leidinggevende. DF&A heeft bovendien aangegeven dat zij in een register bijhouden wie welke data heeft geëxporteerd. Dit register wordt periodiek gecontroleerd door de functionaris dataprotectie van DF&A. Daar komt bij dat wel wordt gelogd welk queryverzoek de betreffende medewerker heeft gedaan. Aan de hand daarvan kan worden achterhaald welke data de medewerker heeft ontvangen binnen de analytische omgeving op de werkplek van de medewerker.

Verder is extern emailverkeer technisch onmogelijk gemaakt voor DF&A en zijn slechts een beperkt aantal vooraf goedgekeurde internetwebsites toegankelijk, waardoor het risico dat data aanwezig bij DF&A buiten de Belastingdienst terecht komt zeer beperkt is.

ii) usb sticks

Dit risico is nog verder beperkt doordat medewerkers geen USB-ontheffing meer krijgen, met uitzondering van beheerders (die daarvoor toestemming moeten vragen bij de verantwoordelijke directeur en de functionaris dataprotectie van DF&A). De bij uitzondering verleende autorisaties aan beheerders worden bijgehouden in een logboek en na gebruik direct ingetrokken.

iii) mobile devices

Het blijkt voor DF&A medewerkers nog wel mogelijk om een bijlage bij een e-mail met gebruik van de 'openen in' functie te openen en op te slaan op mobile devices buiten de beveiligde omgeving van de Belastingdienst. Deze handeling wordt niet gelogd. DF&A geeft aan dat het in zijn algemeenheid niet mogelijk is om de 'openen in' functie te blokkeren, omdat de functionaliteiten die via generieke software en besturingssystemen verlopen niet kunnen worden uitgezet. Voor applicaties die onder 'mobile device management' zijn gebracht geldt dat de 'openen in' functie wel beperkt kan worden, zoals bijvoorbeeld de e-mailapplicatie. DF&A geeft aan dat zij voornemens is de 'openen in' functie voor de applicaties die onder 'mobile device management' vallen op korte termijn waar mogelijk te beperken.

Een mogelijk beveiligingsrisico wordt verder gemitigeerd doordat DF&A medewerkers bijlagen bij e-mails versleuteld moeten versturen. Hierdoor zijn bijlagen op mobile devices niet leesbaar, m.a.w. data op de mobile devices zijn zonder de data te ontsleutelen niet in te zien.

Ad 2) Controle op de logging

Uit de bevindingen van de AP volgt dat DF&A haar logging heeft aangesloten op een systeem waar actieve monitoring plaatsvindt op basis van een achttal triggers[2] die ingericht zijn voor DF&A. Ook het e-mailverkeer van DF&A is aangesloten op dit systeem. Indien vanuit de query opdracht wordt gegeven om het resultaat te mailen naar een niet @belastingdienst.nl adres dan zal dit leiden tot een trigger.[3] Hierop wordt actief gemonitord. DF&A geeft aan dat eerst onderzoek gedaan wordt naar een alert, waarna deze indien nodig doorgezet wordt naar de security officer van DF&A.

Ad 3) Autorisaties

De Belastingdienst heeft aangegeven dat DF&A op basis van doelbinding toegang verleent tot data aan haar medewerkers. Autorisaties van medewerkers zijn gestructureerd per project of datagebied, maar ook op basis van functie en rol binnen het project. Dit is al voor 95% van de data gerealiseerd. Voor het overige deel van de data heeft DF&A toegezegd dat hiervoor inmiddels een technische oplossing is bedacht die geleidelijk ingevoerd zal worden.[4]

Tevens is gebleken dat de verantwoordelijke leidinggevende volgens een vastgestelde procedure handmatig autorisaties van medewerkers ongeldig maakt en de autorisaties maandelijks worden gecontroleerd. Daarbij zouden medewerkers na uitdiensttreding praktisch gezien geen mogelijkheden meer hebben om toegang te krijgen, omdat de werklaptop en Rijkspas ingeleverd worden en het account verwijderd.

Conclusie

De AP concludeert dat de getroffen verbetermaatregelen bij DF&A ten behoeve van de geconstateerde beveiligingsrisico's deze risico's dusdanig verminderen dat de eerder door de AP geconstateerde overtredingen niet langer voortduren.

Deze conclusie is in lijn met recente antwoorden van de staatssecretaris van Financiën[5] en met de uitkomsten in het rapport 'Datagedreven selectie van aangiften door de Belastingdienst' gepubliceerd door de Algemene Rekenkamer.[6] In het rapport van de Rekenkamer wordt ook aangegeven dat medewerkers alleen toegang hebben tot die data die op dat moment nodig is, data opgeslagen wordt in datagebieden die per rol geautoriseerd worden, en een medewerker data niet kan inzien of bewerken zonder op grond van

[2] Een trigger is een geautomatiseerde beslisregel op basis van een uitzondering, ook uitzonderingsregel of exception rule genoemd.
[3] Zie memo 'Monitoring en logging op basis van de exception rules', in de bijlage, onder 6.
[4] Uit de door de AP ontvangen documentatie blijkt dat DF&A een technische oplossing heeft bedacht, namelijk het gebruik van de inputdatabases. Input databases zijn afgescheiden mappen waarin per project alleen die tabellen en kolommen inzichtelijk worden gemaakt, d.m.v. views, die het project nodig heeft. Hierdoor krijgt het project niet automatisch meer toegang tot alle tabellen en kolommen van de datastroom.
[5] TK, 2018-2019, 32 761, nr. 136, 14 juni 2019.
[6] https://www.rekenkamer.nl/publicaties/rapporten/2019/06/11/datagedreven-selectie-van-aangiften-door-de-belastingdienst, d.d. 11 juni 2019.

hun rol geautoriseerd te zijn. Ook vindt actieve monitoring plaats op het gebruik van data door de medewerkers en is het mailen van bestanden naar adressen buiten de Belastingdienst technisch onmogelijk gemaakt. Dit is tevens bevestigd door de staatssecretaris van Financiën.

De AP merkt verder op dat informatiebeveiliging een continu proces is dat vraagt om periodieke evaluatie. Om deze reden wil de AP de Belastingdienst en in het bijzonder DF&A aanmoedigen om:

- audits gericht op informatiebeveiliging te blijven uitvoeren;
- risico's en maatregelen periodiek te herbeoordelen, waaronder bijvoorbeeld het waar mogelijk beperken van de 'openen in' functie van mobile devices.

De AP vertrouwt erop dat DF&A de nodige maatregelen neemt om ervoor te zorgen dat aan de vereisten uit de AVG voldaan blijft worden. Dit geldt ook ten aanzien van alle verplichtingen die niet specifiek in deze brief zijn genoemd. Het niet-naleven van de AVG kan voor de AP aanleiding zijn om over te gaan tot handhaving.

Tot slot

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Voor eventuele vragen kunt u contact opnemen met bovengenoemd contactpersoon.

De AP zendt een afschrift van deze brief aan de Functionaris voor de Gegevensbescherming, de heer J. de Zeeuw. Tevens zendt de AP een afschrift aan de directeur Datafundamenten & Analytics van de Belastingdienst, de heer H. Timmermans.

Hoogachtend,
Autoriteit Persoonsgegevens,

mr. A. Wolfsen
Voorzitter