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

Aangetekend
De Minister van Financiën
De heer mr. W.B. Hoekstra MBA
Korte Voorhout 7
2500 EE DEN HAAG

Datum
3 juli 2018

Ons kenmerk
Z2017-00449

Contactpersoon

Onderwerp
onderzoek naar Data & Analytics

Geachte heer Hoekstra,

In februari 2017 is de Autoriteit Persoonsgegevens een onderzoek gestart naar de informatiebeveiliging van de afdeling Data & Analytics (D&A) van de Belastingdienst. De AP informeert u door middel van deze brief over de resultaten van het onderzoek en over de daarbij geconstateerde overtredingen van de privacyregelgeving. Daarnaast verzoekt de AP u om informatie te verstrekken over de getroffen verbetermaatregelen. Tevens wijst de AP u erop dat u bij het in gebreke blijven van deze verbetermaatregelen handelt in strijd met de wet .

Doel onderzoek

De AP heeft het onderzoek opgedeeld in twee verschillende perioden, te weten de periode van 1 januari 2013 tot en met de periode van 31 december 2016 (onderzoeksperiode I) en de periode van 1 januari 2016 tot en met februari 2017 (onderzoeksperiode II).

Het onderzoek met betrekking tot onderzoeksperiode II richtte zich op de vraag of de Belastingdienst in die periode passende technische en organisatorische maatregelen ten uitvoer heeft gelegd om persoonsgegevens, die werden verwerkt door D&A en haar voorgangers, te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking in de zin van artikel 13 van de Wet bescherming persoonsgegevens (hierna: Wbp). In het bijzonder richtte het onderzoek zich op het verkrijgen van inzicht in de wijze waarop het loggen, de controle op de logging en de toegang tot data (waaronder de autorisatie) bij D&A en haar voorgangers was georganiseerd.

Ten aanzien van onderzoeksperiode I is onderzocht of eventuele gebreken met betrekking tot het loggen, de controle op de logging en autorisaties bij D&A al langer bekend waren bij de Belastingdienst.

Conclusie onderzoek AP

Met betrekking tot onderzoeksperiode I heeft de AP op basis van interne documenten van de Belastingdienst en verklaringen geconstateerd dat er bij D&A ten aanzien van de verwerking van persoonsgegevens tekortkomingen bestonden in de informatiebeveiliging. Die tekortkomingen zagen op de logging, controle op de logging en de autorisaties. Verder is in het onderzoek van de AP naar voren gekomen dat het management op de hoogte was van de tekortkomingen, maar er op dat moment voor heeft gekozen om te wachten met de implementatie van aanvullende technische verbetermaatregelen totdat de migratie van een oud platform naar een nieuw platform was afgerond. Tot die tijd heeft het management ingezet op bewustwording bij D&A medewerkers van het op een juiste manier omgaan met persoonsgegevens.

Ten aanzien van onderzoeksperiode II komt de AP op basis van interne documenten van de Belastingdienst, verklaringen en onderzoek in de loggegevens tot de conclusie dat de geconstateerde tekortkomingen in de informatiebeveiliging die al bestonden in onderzoeksperiode I ook in onderzoeksperiode II nog niet opgelost waren. De AP heeft betreffende drie beveiligingsaspecten geconstateerd die niet in orde waren, te weten:

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

2. De controle op de logging.

3. Het verwijderen/intrekken van autorisaties én te ruime toegangsrechten tot data voor de D&A medewerkers.

Ad 1) De Code voor Informatiebeveiliging[1] (Code) somt een aantal activiteiten op, die voor zover relevant, moeten worden vastgelegd in logbestanden. Het exporteren van data vanuit brongegevens naar de eigen werkplek van een medewerker wordt in de Code aangemerkt als "verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd". Het gebruik en het schrijven van data naar een usb-stick én het opslaan van een bijlage bij een e-mail die wordt geopend op een mobile device zijn aan te merken als "gebruik van systeemmiddelen en –toepassingen".

[1] De Code is een algemeen geaccepteerde technologie-neutrale beveiligingsstandaard binnen de praktijk van informatiebeveiliging Voor de Belastingdienst waren voor de periode van overtreding de standaarden NEN/ISO/IEC 27001: 2013 -en 27001C11+C1+C2 een NEN/ISO27002:2013 -en 27002+C1+C2 van belang. Aan deze NEN-normen wordt gerefereerd als de Code voor Informatiebeveiliging.

Om te beoordelen of de hiervoor beschreven ontbrekende activiteiten kunnen worden aangemerkt als relevante activiteiten, heeft de AP het ontbreken van de logging van die activiteiten in samenhang beoordeeld.

Het ontbreken van 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, levert een risico op voor de beveiliging van die data. Door handelingen op externe gegevensdragers/opslag niet te loggen kan data ongemerkt worden gekopieerd of geëxporteerd. Dit houdt in dat nergens in de keten wordt vastgelegd door wie, welke data mogelijk onrechtmatig buiten de Belastingdienst wordt gebracht. Hierdoor is het ook niet mogelijk om via controle op de logging op te merken dat data via deze weg de Belastingdienst onrechtmatig verlaat. Ook kan achteraf niet worden nagegaan welke data door wie naar buiten is gebracht. Dit tezamen leidt tot de conclusie dat de drie ontbrekende loggingactiviteiten aangemerkt moeten worden als relevante activiteiten. In de betreffende onderzoeksperiode voldeed de Belastingdienst voor wat betreft logging dus niet aan de vereisten van artikel 13 Wbp. De AP heeft hierbij in aanmerking genomen dat gelet op de aard en de omvang[2] van de persoonsgegevens die D&A verwerkt een hoog beveiligingsniveau is vereist voor die verwerking.

Ad 2) Naast het feit dat een aantal relevante activiteiten niet werden gelogd, was de controle op de logging niet in orde. Voor een deel van de logging was deze in zijn geheel niet in orde en voor een ander deel alleen de controle van data die via e-mail buiten de Belastingdienst werd gebracht.

Ad 3) De AP is op basis van haar onderzoek tot de conclusie gekomen dat D&A medewerkers te ruim toegang hadden tot data die niet noodzakelijk was om hun werk te kunnen uitvoeren. Hiermee voldeed de toegangsbeveiliging niet aan de vereisten én aan het principe van 'need-to-know' opgenomen in de Code.

Ten slotte is de AP nagegaan of autorisaties op tijd zijn afgesloten na uit diensttreding van medewerkers of extern ingehuurde medewerkers. Daaruit bleek dat van 100 medewerkers de autorisatie niet onmiddellijk ongeldig was gemaakt of de toegangsrechten waren verwijderd nadat deze medewerkers en extern ingehuurde medewerkers D&A hadden verlaten. De duur van de periode waarin de autorisaties onterecht niet zijn verwijderd/ingetrokken varieerde tussen de 1 en 150 dagen. Overigens is niet gebleken dat D&A medewerkers uit deze groep na hun uit diensttreding nog toegang hebben gehad tot data van D&A doordat hun autorisatie niet op tijd is verwijderd/ingetrokken.

De beschreven uitkomsten van het onderzoek leiden tot de conclusie dat de Belastingdienst voor wat betreft de logging, de controle op de logging en de toegangsbeveiliging bij D&A in strijd handelde met artikel 13 Wbp.

[2] D&A maakt gebruik van de intern beschikbare data van de Belastingdienst en beschikt zo over een grote hoeveelheid aan data, waaronder bijvoorbeeld ook burgerservicenummers.

Datum
3 juli 2018

Ons kenmerk
Z2017-00449

Conclusies onderzoek Belastingdienst

Naast de AP heeft de staatssecretaris van Financiën (staatssecretaris) ook onderzoek laten uitvoeren naar de informatiebeveiliging bij D&A en haar rechtsvoorgangers. Doel van dit onderzoek was om aan de hand van beschikbare loggegevens over gebruik van systemen, applicaties en data bij D&A vanaf de oprichting op 1 februari 2016 tot aanvang van het onderzoek, vast te stellen of getracht is daadwerkelijk gegevens van belastingplichtigen, belastingschuldigen of toeslaggerechtigden buiten de Belastingdienst te brengen. Op 2 oktober 2017 heeft de Belastingdienst de resultaten van de onderzoeken aan de Tweede Kamer gestuurd. Deze resultaten komen overeen met de hierboven beschreven resultaten van het onderzoek van de AP. In het onderzoek van de staatssecretaris zijn bovendien 10 casus geïdentificeerd waarbij persoonsgegevens per e-mail buiten de Belastingdienst zijn terechtgekomen. Dit was niet eerder door de Belastingdienst opgemerkt. Dit kon onopgemerkt blijven door de tekortkomingen in de informatiebeveiliging die, zoals hiervoor beschreven, ook uit het onderzoek van de AP zijn gebleken.

Toezeggingen aan de Kamer

Op 2 oktober 2017 heeft de staatssecretaris de Tweede Kamer per brief geïnformeerd over de resultaten van het door hem geïnitieerde onderzoek naar het gegevensgebruik bij D&A. In de brief heeft de staatsecretaris aangegeven dat "structurele oplossingen voor continue monitoring, pseudonimiseren en datacompartimenteren van de analyseomgeving van D&A op stapel staan". Ten aanzien van het tijdpad voor implementatie is aangegeven dat de eerste actieve monitoring binnen D&A het vierde kwartaal van 2017 wordt gerealiseerd. Implementatie van pseudonimisering/anonimisering zou zijn voorbereid en dat de start op de werkvloer daarvan gepland stond voor het eerste kwartaal 2018 met een doorlooptijd van een jaar. Compartimentering zou volgens de planning medio 2018 gerealiseerd moeten zijn. Dit komt overeen met informatie over de te nemen verbetermaatregelen verstrekt door de staatssecretaris aan de AP per brief van 7 augustus 2017.

Gewenste informatie over getroffen verbetermaatregelen

Gelet op de toezeggingen over de te nemen verbetermaatregelen die de staatsecretaris heeft gedaan aan de Tweede Kamer acht de AP daarom voortzetting van het onderzoek resulterend in een afzonderlijk onderzoeksrapport niet langer opportuun om ervoor te zorgen dat de Belastingdienst haar handelwijze in overeenstemming brengt met de vereisten van de AVG.

Voorgaande neemt niet weg dat bij het in gebreke blijven van de Belastingdienst om de toegezegde verbetermaatregelen te implementeren, de minister van Financiën in de hoedanigheid van verantwoordelijke onder de AVG, nog steeds in strijd met de wet handelt. Het onderzoek dat de AP heeft verricht naar de tekortkomingen in de beveiliging bij D&A zag op een periode waarin de Algemene Verordening Gegevensbescherming (AVG) nog niet van kracht was. De aard en strekking van de norm die is neergelegd in artikel 32 van de AVG (waarin is opgenomen waaraan de beveiliging van de verwerking van persoonsgegevens moet voldoen) komt overeen met de aard en de strekking van de norm van artikel

Datum
3 juli 2018

Ons kenmerk
Z2017-00449

13 van de Wbp. De AP verzoekt de Minister dan ook uiterlijk 1 augustus 2018 een rapportage te verstrekken met een beschrijving van de stand van zaken ten aanzien van de verbetermaatregelen genoemd in de eerder aangehaalde brief van de staatssecretaris van 2 oktober 2017. Op basis daarvan bepaalt de AP of aanvullend onderzoek nodig is. Bij de beslissing daaromtrent wordt meegewogen dat de staatssecretaris in antwoord op Kamervragen van 5 juni 2018 heeft aangegeven dat er bij de Belastingdienst een aantal tekortkomingen in de naleving van de AVG is geconstateerd. De in die brief genoemde tekortkomingen overlappen deels met de tekortkomingen die de AP in haar onderzoek naar D&A heeft geconstateerd. Mogelijk dat het aanvullend onderzoek dan breder wordt getrokken. Als uit dat onderzoek blijkt dat de eerder bij de afdeling D&A geconstateerde overtredingen niet beëindigd zijn, dan zal de AP niet schromen om handhavingsmiddelen in te zetten die ons ten dienste staan.

De AP zendt een afschrift van deze brief aan de Functionaris voor de Gegevensbescherming, de heer de Zeeuw.

Deze brief betreft geen besluit in de zin van artikel 1:3 van de Algemene wet bestuursrecht. Derhalve staan hiertegen geen rechtsmiddelen open.

Indien u naar aanleiding van deze brief nog vragen heeft, kunt u contact opnemen met bovengenoemd contactpersoon.

Hoogachtend,
De Autoriteit Persoonsgegevens,

Mr. A. Wolfsen
Voorzitter