Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

De voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal
Belastingdienst

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

Ons kenmerk
2019-0000218975

Uw brief (kenmerk)

Datum	27 februari 2020
Betreft	Inbreng Schriftelijk Overleg over eindbrief van de Autoriteit Persoonsgegevens over het onderzoek naar de informatiebeveiliging bij de afdeling Datafundamenten en Analytics van de Belastingdienst

Geachte voorzitter,

Hierbij stuur ik u de antwoorden op de schriftelijke vragen van de vaste commissie voor Financiën zoals gesteld op 29 november 2019 naar aanleiding van de brief van 16 oktober 2019 inzake de eindbrief van de Autoriteit Persoonsgegevens over het onderzoek naar de informatiebeveiliging bij de afdeling Datafundamenten en Analytics van de Belastingdienst (Kamerstuk 32 761, nr. 150).

Hoogachtend,

De staatssecretaris van Financiën – Fiscaliteit en Belastingdienst

J.A. Vijlbrief

De vaste commissie voor Financiën heeft op 29 november 2019 een aantal vragen en opmerkingen voorgelegd aan de (toenmalige) staatssecretaris van Financiën over zijn brief van 16 oktober 2019 inzake de eindbrief van de Autoriteit Persoonsgegevens over het onderzoek naar de informatiebeveiliging bij de afdeling Datafundamenten en Analytics van de Belastingdienst (Kamerstuk 32 761, nr. 150).

II Reactie van de staatssecretaris – Fiscaliteit en Belastingdienst

Ik dank de leden van de fracties van de VVD, het CDA en de SP voor de gestelde vragen naar aanleiding van de brief van 16 oktober 2019 van mijn ambtsvoorganger. Hierna zal ik de vragen per fractie beantwoorden. Daarbij wordt zoveel mogelijk de volgorde van het verslag gevolgd, behalve daar waar fracties een overeenkomende vraag hebben gesteld.

Antwoorden op de vragen en opmerkingen van de leden van de fractie van de VVD

De leden van de VVD-fractie hebben kennisgenomen van de brief 'Onderzoek van de AP naar de informatiebeveiliging bij Belastingdienst/Datafundamenten en Analytics' en zijn tevreden met het feit dat de Belastingdienst en de afdeling Datafundamenten & Analytics (DF&A) volgens de Autoriteit Persoonsgegevens (AP) voldoende verbetermaatregelen hebben getroffen ten behoeve van de eerder geconstateerde beveiligingsrisico's. De leden van de VVD-fractie hebben nog enkele vragen en opmerkingen.

De leden van de VVD-fractie hechten eraan te benadrukken dat de Belastingdienst dient te voldoen aan de hoogste eisen voor wat betreft databescherming en de beveiliging van de privacy van gevoelige gegevens van Nederlanders. Zij vragen het kabinet hier blijvend aandacht aan te besteden.
Dat zal ik doen.

De leden van de VVD-fractie vragen of de AP alleen heeft gekeken naar de eerder geconstateerde beveiligingsrisico's of dat DF&A in zijn geheel opnieuw is onderzocht op beveiligingsrisico's. Zo ja, wat is de uitkomst?
De AP heeft primair gekeken naar de geconstateerde beveiligingsrisico's, zoals die gecommuniceerd zijn in de brief van de AP van 3 juli 2018[1], en de getroffen verbetermaatregelen. De AP heeft in haar onderzoek ook de bevindingen van een intern onderzoek en van het onderzoek 'Datagedreven selectie van aangiften door de Belastingdienst' van de Algemene Rekenkamer[2], en de daarbij behorende getroffen verbetermaatregelen, meegenomen. De uitkomsten van dit onderzoek, waarbij ook de andere bevindingen zijn meegenomen, kunt u lezen in de eindbrief van de AP van 14 oktober 2019, die op 16 oktober 2019 aan uw Kamer gestuurd is. De AP concludeert in de eindbrief 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* […]".

De leden van de VVD-fractie lezen dat exportdata nog steeds niet wordt gelogd. Op welke manier kan in een register worden bijgehouden wie welke data heeft geëxporteerd? Moeten medewerkers zelf aangeven welke data is geëxporteerd?

[1] Kamerstukken II, 2018/19, 32 761, nr. 125; bijlage bij de brief van 28 september 2018

[2] Kamerstukken II, 2018/19, 31 066, nr. 488

Deze vraag is reeds beantwoord in de brief aan de Kamer van 14 juni 2019.[3] Ik citeer : *[…] De leden van de fractie van het CDA vragen in verband met een data «check out» hoe de procedure voor een zorgvuldige omgang met de gegevens procedure eruitziet. Binnen de corporate dienst Datafundamenten en Analytics (verder: DF&A) wordt middels diverse programma's voortdurend aandacht besteed aan bewustwording rondom gegevensbescherming. Vanaf januari 2019 geldt de procedure dat een medewerker toestemming moet vragen aan zijn leidinggevende als de exportfunctie of de copy-paste-functie in de analyse-software wordt gebruikt. De leidinggevende registreert dit in een centraal register. In de maandrapportage komen de aantallen terug. Door de maatregelen is het niet mogelijk gegevens na een «check out» verder te exporteren. Er vindt geen 100% logging plaats, maar registratie door de leidinggevende van de toestemming. Ik vind het belangrijk om te benadrukken dat opzettelijke misbruik helaas nooit helemaal te voorkomen is. Uiteraard spant de Belastingdienst zich in om dit zoveel mogelijk te voorkomen. […]*

De leden van de VVD-fractie vragen of binnen de Belastingdienst de verbetermaatregelen rond de geconstateerde gebreken breed aangepast zijn of dat dit alleen voor DF&A is gebeurd.
Daar waar medewerkers gebruik maken van analyse-tooling en ten behoeve daarvan rechtstreeks toegang nodig hebben tot brondata, zijn de verbetermaatregelen toegepast.

Op basis waarvan wordt besloten om internetwebsites wel of niet goed te keuren?
De aangevraagde website wordt beoordeeld op het hebben van de mogelijkheid tot data-export zoals webmail en mogelijkheden voor bestandsoverdracht, zoals die geboden worden door o.a. Dropbox, WeTransfer etc. Alleen websites die niet beschikken over deze functionaliteit worden goedgekeurd.

De leden van de VVD-fractie vragen wie er binnen de Belastingdienst op toeziet dat de getroffen verbetermaatregelen en periodieke herbeoordeling in de toekomst worden gecontinueerd. Worden er nog 'nazorgcontroles' gedaan door de AP? Zo ja, met welke regelmaat? Zo nee, waarom niet?
Informatiebeveiliging is een continu proces. Periodiek worden bestaande maatregelen beoordeeld op effectiviteit en worden de risico's opnieuw in kaart gebracht. Waar nodig worden nieuwe risico's gemitigeerd door nieuwe maatregelen. Dit proces staat onder toezicht van de chief information and security officer (CISO) van de Belastingdienst en de beveiligingsambtenaar (BVA) en de functionaris voor gegevensbescherming (FG) van het ministerie van Financiën. Het proces kan worden geaudit door de ADR. De AP heeft haar eigen werkwijze. Mijn ervaring is dat wanneer de AP bepaalde feiten constateert, zij deze onderzoekt en dat de AP op een later moment onderzoekt of bij een eventueel vastgestelde overtreding afdoende maatregelen genomen zijn zodat de geconstateerde overtreding niet langer voortduurt.

De leden van de VVD-fractie lezen dat de Belastingdienst naar aanleiding van het onderzoek van de Algemene Rekenkamer pas het mailen van DF&A naar buiten de Belastingdienst onmogelijk heeft gemaakt. Hoe is de informatiebeveiliging op andere afdelingen binnen de Belastingdienst? Kan op andere privacygevoelige afdelingen ook geen mail naar buiten de Belastingdienst gemaild worden? Waarom wel/waarom niet?

[3] Kamerstukken II, 2018/19, 32 761, nr. 136

De Belastingdienst heeft de informatiebeveiliging niet ingericht per afdeling. De Belastingdienst beschermt alle gegevens met maatregelen op basis van risicoanalyses, conform de vereisten uit Baseline Informatiebeveiliging Overheid (BIO), niveau BBN2. Bij het gebruik van internet en extern e-mailen wordt van alle medewerkers verwacht professioneel en integer te handelen. Hiervoor gelden de uitgangspunten die op elke rijksambtenaar van toepassing zijn. Het dichtzetten van de e-mail bij de voorgangers van DF&A, de Broedkamer c.q. D&A, was onderdeel van een noodmaatregel, omdat ten tijde van het incident onduidelijk was hoe de gegevens van de Belastingdienst 'buiten de deur' terecht gekomen waren. Op basis van het onderzoek is vervolgens besloten deze maatregel in stand te houden voor medewerkers die toegang hebben tot de bronbestanden in een analyse-omgeving. Deze overweging is gemaakt op basis van een risicoanalyse. Privacy is één van de risico's die daarin meegenomen wordt. De maatregel geldt voor alle analyseprocessen binnen de Belastingdienst, waarbij toegang is tot bronbestanden.

De leden van de VVD-fractie vragen hoe de AP blijft monitoren of DF&A de verbetermaatregelen voldoende continueert en hoe de AP toeziet op het naleven van de Algemene verordening gegevensbescherming (AVG).
De AP is de nationale toezichthouder voor de naleving van de regels voor gegevensbescherming. De AP bepaalt zelf op welke wijze toezicht gehouden wordt.

De leden van de VVD-fractie vragen om een uitputtende lijst van diensten of afdelingen binnen de Belastingdienst die op dit moment nog niet voldoen aan de laatste privacywetgeving zoals de AVG. Zij vragen daarnaast welke stappen de Belastingdienst zet om wel aan deze wet- en regelgeving te voldoen en wanneer de Belastingdienst volledig 'privacyproof' zal zijn.
Mijn ambtsvoorganger heeft in de brief aan uw Kamer van 28 mei 2019[4] aangegeven dat de Belastingdienst de maatregelen om de AVG te implementeren heeft kunnen realiseren, met uitzondering van de maatregel 'verwijderen van verouderde gegevens'. Om te voorkomen dat de niet-tijdig verwijderde gegevens onrechtmatig kunnen worden verwerkt, heeft de Belastingdienst mitigerende maatregelen genomen: een zogenoemde datakluis, waardoor de toegang tot de persoonsgegevens wordt weggenomen. In de brief is de toezegging gedaan de Auditdienst Rijk (ADR) te vragen te toetsen in hoeverre de Belastingdienst zijn oorspronkelijke aanbevelingen heeft opgevolgd.

Het aanvullend onderzoek door de ADR is afgerond. Als bijlage bij deze brief stuur ik u het rapport. De centrale boodschap van de ADR is dat de Belastingdienst met de aanbevelingen aan de slag is gegaan, maar dat er nog vervolgacties nodig zijn om alle bevindingen volledig op te lossen. Het voorgaande leidt tot het inzicht dat er nog meer maatregelen genomen moeten worden dan in mei 2019 aan de Tweede Kamer is gecommuniceerd. Hoewel de Belastingdienst een grote inspanning heeft geleverd om te kunnen voldoen aan de AVG, is hiermee duidelijk geworden dat er meer focus moet komen op het realiseren van de resterende aanbevelingen. De resterende aanbevelingen zijn:
- Het aantoonbaar afhandelen van de lijst met de Belastingdienst-applicaties die voorzien zijn van een bulkexportfaciliteit;
- Het compleet maken en actualiseren van de verwerkersovereenkomsten in het AVG-register;

[4] Kamerstukken II, 2018/19, 31 066, nr. 485

- Werkinstructies voor 'gebruik productiedata in test' nader uitwerken;
- Het ontwikkelen en implementeren van de kaders om tot meer uniforme inrichting van bedrijfsrollen te komen.

Het realiseren van de eerste drie resterende aanbevelingen zal maximaal zes maanden duren. Het ontwikkelen en implementeren van uniforme inrichting bedrijfsrollen is al gestart, maar de realisatie daarvan zal langer duren.

Naleving van de AVG is overigens geen statisch gegeven, maar een proces dat voortdurend aandacht vergt. De genomen maatregelen en de gestelde kaders moeten worden onderhouden. De Belastingdienst blijft dus doorlopend werken aan maatregelen en kaders en streeft daarmee naar een duurzame naleving van de AVG. Voor 2020 staan verschillende acties gepland. Zo wordt er gewerkt aan de kwaliteitsverbetering van het register van verwerkingen; daartoe wordt een plan van aanpak opgesteld. De functionaris voor gegevensbescherming is overigens voornemens in 2020 een audit te laten doen op het register van verwerkingen. Ook wordt in 2020 de rol van de zogenoemde datacoördinatoren geëvalueerd. Ik vind het belangrijk om te benadrukken dat incidenten niet zijn uit te sluiten, in de veelheid van (veranderende) processen en complexiteit van de organisatie. De Belastingdienst handelt deze situaties conform de normen van de AVG af.

Antwoorden op de vragen en opmerkingen van de leden van de fractie van het CDA

De leden van de CDA-fractie danken de staatssecretaris en de AP voor de brief over de informatiebeveiliging bij de broedkamer, die nu DF&A heet. Het is goed dat de verbetermaatregelen genomen zijn en dat de AP niet langer overtredingen gevonden heeft.

Toch is hiermee wat de leden van de CDA-fractie betreft de zaak niet helemaal afgesloten. Daarvoor waren de constateringen, die in de uitzending van Zembla naar boven kwamen, te ernstig.

Graag willen de leden van de CDA-fractie weten welke maatregelen nu uiteindelijk genomen zijn op personeel terrein en op institutioneel terrein. Bij de tweede vraag willen de leden ook graag vernemen waar medewerkers problemen met de AVG en privacy kunnen melden en hoe daarmee wordt omgegaan.

Er is een uitgebreide bewustwordingscampagne voor alle medewerkers (intern en extern) van DF&A. Deze bestaat uit:
- dagdeel plenaire cursus Privacy en Security, speciaal ontwikkeld voor medewerkers van DF&A (verplicht);
- online cursus "iBewustzijn Overheid" (verplicht);
- online cursus "Basistraining Privacy en AVG" (verplicht);
- de 10 'gouden regels' van DF&A;
- aanwijzen van een eigen vertrouwenspersoon;
- op afdelingsbrede en teamoverleggen regelmatig aandacht voor privacybescherming door bespreken casuïstiek en quizelementen.

Op organisatorisch vlak heeft DF&A de afgelopen jaren de volgende maatregelen getroffen ter beveiliging van de gegevens van burgers en bedrijven door het (verder) implementeren van beveiligingsmaatregelen:

- DF&A analyseert de risico's en de besturing van het risico-managementproces is verbeterd;
- er wordt voor DF&A verbijzonderde toegangsbeveiliging toegepast;
- DF&A hanteert eerder genoemde 'gouden regels' en trainingen om het beveiligingsbewustzijn te vergroten;
- er vindt monitoring plaats op het naar buiten de Belastingdienst brengen van gegevens;
- er vindt binnen DF&A monitoring plaats op toegekende autorisaties, conflicterende mutatierechten en USB-rechten;
- conform de vereisten van de AVG is *privacy by design* geïmplementeerd binnen de organisatie. Dit is een manier van werken waarbij al vanaf de start van het project over privacy wordt nagedacht en dit gedurende het gehele project wordt meegenomen en waar nodig aangepast aan de situatie;
- de data-analyseomgeving is ingericht met functiescheiding en projectgebonden autorisaties; in de uitvoering wordt soms op meerdere projecten autorisaties verstrekt;
- er zijn diverse maatregelen getroffen om datatransfer van de data-analyse-omgeving naar buiten de Belastingdienst te voorkomen.

Medewerkers kunnen met vragen op het gebied van privacy terecht bij contactpersonen binnen hun eigen dienstonderdeel, zogenoemde datacoördinatoren. Voor de Belastingdienst in brede zin is er een privacyofficer. Daarnaast beschikt het ministerie van Financiën, inclusief de Belastingdienst, over een functionaris voor gegevensbescherming (FG). De FG is een interne toezichthouder voor de naleving van de regels van de AVG. De Autoriteit Persoonsgegevens is de nationale, externe, toezichthouder.

Ook wijs ik op het belang van cultuur.[5] Aandacht voor de cultuur bij de Belastingdienst is van groot belang om de wezenlijke veranderopgaven te kunnen realiseren. Daarom is cultuur tot een van de pijlers van Beheerst Vernieuwen gemaakt en is het bestaande cultuurprogramma geïntensiveerd en uitgebreid als stevig en niet vrijblijvend programma. Een klimaat is nodig waar fouten op het juiste niveau worden gemeld, nadrukkelijk van die fouten wordt geleerd, dilemma's worden besproken en moreel leiderschap en rechtstatelijk handelen de mores zijn. Misstanden moeten vrijelijk gemeld kunnen worden en op een juiste manier opvolging krijgen.

De leden van de CDA-fractie willen de staatssecretaris wel op het hart drukken dat de AVG niet betekent dat oude documenten (zoals memo's en beleidsdocumenten) waarop namen van ambtenaren staan, vernietigd dienen te worden. Kan de staatssecretaris bevestigen dat dat niet gebeurt?
Het vernietigen van documenten gebeurt conform de vereisten uit de Archiefwet, waarbij de termijnen van de selectielijsten[6] gehanteerd worden. Het gaat hierbij om integrale gegevens; er worden tussentijds geen persoonsgegevens van ambtenaren verwijderd. Zoals eerder aangegeven heeft de Belastingdienst een achterstand bij het schonen van gegevens. Gegeven de hoeveelheid te beoordelen documenten heeft de Belastingdienst als mitigerende maatregel de datakluis ontworpen, waardoor de toegang tot de persoonsgegevens wordt weggenomen.

[5] https://www.rijksoverheid.nl/documenten/kamerstukken/2020/01/11/kamerbrief-versterken-besturing-belastingdienst
[6] https://www.nationaalarchief.nl/archiveren/kennisbank/vastgestelde-selectielijsten

Overigens is in overdrachtsbrief CAF Toeslagen van 4 februari 2020 gemeld dat de Inspectie Overheidsinformatie en Erfgoed (hierna: Inspectie O&E) heeft aangegeven zich op de hoogte te willen stellen van de archivering van informatie in het proces van de toeslagen kinderopvang bij de Belastingdienst. De Inspectie O&E houdt toezicht op de naleving van de Archiefwet 1995 bij de centrale overheid. De beoogde reikwijdte van het aangekondigde onderzoek wordt momenteel met de Inspectie O&E besproken. Hierbij wordt, conform de toezegging aan de heer Omtzigt tijdens het debat van 21 januari 2020, ook de mogelijkheid van een rol van de Rijksarchivaris betrokken.

De leden van de CDA-fractie noemen dat DF&A een schat aan informatie heeft over elke burger. Onder de AVG heeft elke burger ook het recht om die in te zien. Kan de staatssecretaris aangeven hoe een burger al die data op gemakkelijke wijze kan inzien? Nu kan hij namelijk die data niet via de portal inzien.
In de brief van 7 februari 2019[7] aan uw Kamer heb ik aangegeven dat op de website van de Belastingdienst de procedure beschreven is hoe een burger gebruik kan maken van zijn inzagerecht.[8] Ik merk hierbij op dat een burger specifiek naar een verwerking of naar een organisatieonderdeel kan vragen bij een verzoek om inzage.

Vragen en opmerkingen van de leden van de fractie van de SP

De leden van de SP-fractie lezen in de brief van de AP dat zij afdoende vertrouwen heeft in de door de Belastingdienst getroffen maatregelen om de in het verleden voorkomende overtredingen niet langer te laten voortduren. Deze leden lezen tevens in deze brief dat de AP audits gericht op informatiebeveiliging en periodieke herbeoordeling van risico's en maatregelen daartegen voorschrijft. Zij merken tevens op dat de staatssecretaris toezegt in zijn brief dat de Belastingdienst dit zal doen. Deze leden vragen de staatssecretaris hoe dit gestalte gaat krijgen en daarbij specifiek in te gaan op de frequentie en omvang van de audits en tevens op de frequentie van herbeoordeling van risico's binnen DF&A.
De door de AP voorgeschreven audits en periodieke herbeoordeling van de risico's en maatregelen zijn onderdeel van de reguliere 'planning en control'-cyclus. Vanuit de wettelijke taak van de ADR, de aansluitvoorwaarden voor het gebruik van DigiD en vraaggestuurde audits op basis van de rapportages van de bedrijfsonderdelen vinden jaarlijks verschillende audits plaats op (delen van) het verplicht te hanteren kader voor informatiebeveiliging, de BIO. Daarnaast vindt er intern toezicht plaats door de beveiligingsambtenaar van het departement van Financiën.

Tot slot vragen deze leden of de staatssecretaris van zins is de AP en eventuele andere onafhankelijke toezichthouders periodiek controle te laten uitvoeren om te bezien of het vertrouwen dat in haar onderzoek is uitgesproken gerechtvaardigd blijkt.
De Belastingdienst hanteert het Beveiligingsvoorschrift Rijksdienst en het bijbehorende Voorschrift Informatiebeveiliging Rijksdienst voor de inrichting en besturing van informatiebeveiliging. Genoemde kaders bevatten voldoende instrumenten om het gevraagde toezicht uit te voeren.

[7] Kamerstukken II, 2018/19, 32 761, nr. 131

[8] https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/niet_in_enig_menu/prive/privacy