Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

32 761 Verwerking en bescherming persoonsgegevens

Nr. 131

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 8 februari 2019

De vaste commissie voor Financiën heeft een aantal vragen en opmerkingen voorgelegd aan de Staatssecretaris van Financiën over de brief van 28 september 2018 over de reactie op verzoek commissie inzake onderzoek van de Autoriteit Persoonsgegevens naar de informatiebeveiliging van de afdeling Data en Analytics van de Belastingdienst (Kamerstuk 32 761, nr. 125).

De vragen en opmerkingen zijn op 2 november 2018 aan de Staatssecretaris van Financiën voorgelegd. Bij brief van 7 februari 2019 zijn de vragen beantwoord.

De voorzitter van de commissie,
Anne Mulder

De adjunct-griffier van de commissie,
Freriks

kst-32761-131
ISSN 0921 - 7371
's-Gravenhage 2019

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de fractie van de VVD

De leden van de VVD-fractie hebben kennisgenomen van de reactie van de Belastingdienst op het onderzoek van de AP bij de Belastingdienst. Zij hebben nog wel enkele vragen en opmerkingen.

De leden van de VVD-fractie lezen dat de AP geen aanleiding ziet om een officieel onderzoeksrapport uit te brengen, terwijl de Directeur-Generaal (DG) van de Belastingdienst toegeeft dat het voor de Belastingdienst technisch onmogelijk is de privacy van de Nederlanders volledig te waarborgen. Kan de Staatssecretaris de Kamer op de hoogte brengen van de redenen van de AP om geen onderzoeksrapport uit te brengen?

De AP heeft geconstateerd dat er bij D&A ten aanzien van de verwerking van persoonsgegevens tekortkomingen bestaan in de informatiebeveiliging. Dit baart de leden van de VVD-fractie zorgen, aangezien dit niet alleen gevolgen heeft voor de privacy, maar ook voor de inning van belastinggeld in het algemeen, alsook de cybersecurity van de Belastingdienst in het algemeen. Herkent de Staatssecretaris zich in de zorgen van de leden van de VVD-fractie? Of is de Staatssecretaris van mening dat de tekortkomingen met de maatregelen zijn verholpen? Zo ja, hoe verklaart de Staatssecretaris dan de woorden van de DG van de Belastingdienst dat het technisch onmogelijk is de privacy 100% te beveiligen/garanderen? Zo nee, waarom niet?

De Belastingdienst geeft aan dat het technisch onmogelijk is om persoonsdata te beveiligen. De leden van de VVD-fractie vragen zich af welke technische onmogelijkheden dit precies zijn.
Verwacht de Staatssecretaris dat technische onmogelijkheden bij het beveiligen van persoonsgegevens kunnen worden opgelost? Zo nee, waarom niet? Zo ja, welke stappen moeten naast bovengenoemde nog gezet worden?

De leden van de VVD-fractie vragen of er tussen 2 oktober 2017 en oktober 2018 nog casussen bekend zijn waarbij persoonsgegevens per e-mail of andere communicatiemiddelen buiten de Belastingdienst terecht zijn gekomen.

De leden van de VVD-fractie vragen waarom het management van de Belastingdienst heeft gewacht met het implementeren van aanvullende technische verbetermaatregelen terwijl de gegevens en privacy van vele Nederlanders niet gegarandeerd konden worden. Was de Staatssecretaris op de hoogte van de tekortkomingen? Zo ja, is de Staatssecretaris het met deze leden eens dat de Kamer hierover geïnformeerd had moeten worden? Zo nee, waarom niet?

De leden van de VVD-fractie vragen wat de Belastingdienst doet bij overtreding van de procedures omtrent het schrijven van data op een USB-stick. Wie heeft er allemaal toegang tot het genoemde register?

De leden van de VVD-fractie vragen hoeveel trainingen en bewustwordingssessies de medewerkers van de Belastingdienst jaarlijks volgen. Wat wordt er zoal besproken wat betreft de privacygegevens van Nederlanders en de veiligheid van gegevens van de Belastingdienst?
Sinds wanneer is de controle op «logging» binnen D&A operationeel? Heeft dit al geleid tot het afgaan van «triggers»? Zo ja, wat is er vervolgens met deze signalen gebeurd?

De leden van de VVD-fractie vragen waarom de Belastingdienst heeft gekozen voor een audit door interne auditors met betrekking tot de beveiligingsonderzoeken. Is de Staatssecretaris het met deze leden eens dat dit lijkt alsof de slager zijn eigen vlees keurt? Hoe staat de Staatssecretaris tegenover een audit door de Auditdienst Rijk?

De leden van de VVD-fractie vragen of de Staatssecretaris de Kamer kan informeren over de voortgang met betrekking tot het voldoen aan de Algemene verordening gegevensbescherming (AVG). Zal de gehele Belastingdienst, zoals eerder toegezegd door de Staatssecretaris, eind 2018 voldoen aan een AVG-compliant situatie?
De Autoriteit Persoonsgegevens verwijst naar een aantal tekortkomingen in de naleving van de AVG. Kan de Staatssecretaris de Kamer per tekortkoming informeren over de genomen maatregelen om deze tekortkomingen te verhelpen?

De leden van de VVD-fractie merken op dat de Belastingdienst privacygegevens van Nederlanders niet 100% kan beveiligen. Heeft de Belastingdienst wel 100% inzicht in de beschikbare data?

De leden van de VVD-fractie constateren dat het onderzoek van de Autoriteit Persoonsgegevens gericht was op de afdeling D&A van de Belastingdienst. Heeft de Belastingdienst de maatregelen ter verbetering van de privacygegevens ook doorgevoerd op andere afdelingen? Zo ja, op welke? Zo nee, kunnen de leden van de VVD-fractie hieruit concluderen dat de andere afdelingen van de Belastingdienst de persoonsgegevens 100% kunnen beveiligen?

Vragen en opmerkingen van de leden van de fractie van het CDA

De leden van de CDA-fractie hebben met verbazing de brief van de Staatssecretaris gelezen. Zij kunnen deze paragraaf niet plaatsen:
«De AP concludeert in zijn brief dat zijn bevindingen overeenkomen met de bevindingen uit de onderzoeken die de Belastingdienst zelf heeft uitgevoerd naar de informatiebeveiliging bij de Broedkamer en D&A. Omdat naar aanleiding daarvan ook al maatregelen zijn genomen, ziet de AP geen aanleiding om nog een officieel onderzoeksrapport uit te brengen.»
Handhaaft de Staatssecretaris deze paragraaf in de brief of niet, zo vragen de leden van de CDA-fractie.

De leden van de CDA-fractie verzoeken de Staatssecretaris ook het rapport van eerste bevindingen aan de Kamer te doen toekomen, een verzoek dat zij overigens al meerdere malen in de commissie gedaan hebben.

Ook zouden de leden van de CDA-fractie graag de reactie van de AP op de brief van de DG ontvangen. Deze leden kunnen zich namelijk niet voorstellen dat de AP ook maar in de verste verte gerust gesteld is door het antwoord van de Belastingdienst.
De reden is natuurlijk duidelijk. De brief van de DG van de Belastingdienst schetst een onthutsend beeld van de verbeteringen. Is de Staatssecretaris bereid om alle toezeggingen over de Broedkamer die zijn gedaan bij het debat over de Belastingdienst op 9 februari 2017[1], het algemeen overleg over de Herijking Investeringsagenda Belastingdienst van 25 oktober 2017[2] en de brief van 2 oktober 2017[3] op een rij te zetten en aan te geven of ze zijn opgevolgd?

---

[1] Handelingen II 2016/17, nr. 51, items 5 en 8.
[2] Kamerstuk 31 066, nr. 386.
[3] Kamerstuk 31 066, nr. 379.

De leden van de CDA-fractie zijn ook verbaasd dat D&A nu als AVG-compliant wordt beschouwd. Graag ontvangen deze leden hiervan een auditrapport.
Indien er AVG-compliantie is, dan bestaat er natuurlijk ook inzagerecht en vergeetrecht (immers niet alle data zijn noodzakelijk voor de primaire processen).
Is de Belastingdienst bereid om aan te geven waar een burger of bedrijf kan vragen welke data D&A over hem/haar heeft en hoe hij/zij daar inzage in kan krijgen? Hoeveel mensen hebben al inzage gekregen in de persoonlijke data bij D&A?

De leden van de CDA-fractie hebben ook nog een aantal specifieke vragen:
Hoe is de «werkplek van een medewerker» vormgegeven? Mogen individuele analisten een data «check out» doen naar een lokale omgeving? Zo ja, kan die omgeving op een server zijn of ook op desktop of een mobiel device? Welke exportfunctie van data is aanwezig en waarom kan daarop nog steeds niet gelogd worden?
Waarom is het niet technisch onmogelijk gemaakt om data op een USB-stick te zeten? Vindt er op dit moment logging plaats van het exporteren van data naar een USB-stick (met of zonder autorisatie)?

Welke meldingen van gegevenslekken hebben de Broedkamer en haar rechtsopvolgers de afgelopen vijf jaar gedaan? Kan de Staatssecretaris hiervan een overzicht geven?
Wat is het tijdspad voor pseudonimisering? Bestaat er algemene logging binnen de applicaties van de Broedkamer, wie (naam en rugnummer), verricht welke handelingen (opdrachten/queries) en benadert welke data? Zijn er ooit aanwijzingen gevonden dat er data naar buiten de Belastingdienst is geëxporteerd, bijvoorbeeld bij de politie?
Hoe is op dit moment de logging van de export van data vanuit de brongegevens?
Tot slot vernemen de leden van de CDA-fractie graag welke vorderingen de Belastingdienst in zijn algemeenheid heeft geboekt voor het bereiken van AVG compliantie.

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

De leden van de SP-fractie hebben kennisgenomen van de reactie op het onderzoek van de AP bij de Belastingdienst. Deze leden vinden dat als er ergens goede persoonsbeveiliging moet zijn, het wel bij de Belastingdienst is. Het baart deze leden zorgen dat in de begeleidende brief aan de Kamer enkel wordt weergegeven dat de AP hetzelfde constateerde als eerder onderzoek, maar dat niet de gelegenheid is genomen om de Kamer te informeren over de stand van zaken met betrekking tot de grote privacyproblemen die het eerdere onderzoek constateerde.

De leden van de SP-fractie nemen met zorg kennis van de brief van de AP, d.d. 3 juli 2018, en de reactie van het ministerie daarop, d.d. 19 september 2018. Uit de correspondentie, alsmede de op 6 juni 2018 beantwoorde Kamervragen van het lid Omtzigt (Aanhangsel Handelingen II 2017/18, nr. 2345) komen wat de leden van de SP-fractie betreft een aantal zorgelijke situaties naar voren. Allereerst willen zij de Staatssecretaris erop wijzen dat persoonsgegevens zeer lucratief kunnen zijn als die in verkeerde handen vallen. Het is zorgelijk dat zo een belangrijke overheidsdienst als de Belastingdienst maar liefst een jaar de tijd nodig heeft om aan de AVG te voldoen. Kan de Staatssecretaris aangeven of dit nog steeds als haalbare termijn wordt gezien of is er inmiddels vertraging opgelopen en zo ja, op welke onderdelen precies?

Allereerst maken de leden van de SP-fractie zich zorgen om het feit dat niet wordt bijgehouden welke gegevens door medewerkers worden opgevraagd. Deze leden vragen de Staatssecretaris wanneer de Belastingdienst kan garanderen dat gevoelige persoonsgegevens niet buiten de systemen belanden. Voorgenoemde leden vinden het terecht dat bij gebrek aan het kunnen aanpassen van autorisaties aan bewustwording wordt gedaan, maar zij maken zich zorgen dat via mobiele devices nog altijd bijlagen kunnen worden opgeslagen. Wat houden de genoemde sancties op kwaadwillende acties precies in? Hoe waterdicht is het sanctieregime en is dat afdoende om te voorkomen dat er toch gegevens worden opgeslagen en mogelijk de dienst onterecht verlaten? Is het bijvoorbeeld mogelijk dat er via mobile devices bestanden gemaild kunnen worden naar buiten de dienst?

De leden van de SP-fractie hebben gezien dat de controle op de logging inmiddels operationeel is en vragen de Staatssecretaris wat er bedoeld wordt met de acties die voortkomen uit triggers die zijn vormgegeven. Kan de Staatssecretaris voorbeelden geven van wat een trigger is en hoe er dan wordt opgetreden? Is het mogelijk dat er op papier goede processen zijn beschreven, maar dat die in de praktijk niet opgevolgd worden? Hoe wordt dit voorkomen?

Als het gaat om de autorisaties en toegangsrechten vragen de leden van de SP-fractie of het mogelijk is dat een medewerker die de Belastingdienst verlaat toch nog maximaal 30 dagen toegang heeft, omdat eens per maand een volledige check wordt uitgevoerd. Zou het niet beter zijn dat wanneer iemand uit dienst treedt of elders bij de Belastingdienst gaat werken de autorisaties standaard betrokken worden en per direct worden omgezet? Kan de Staatssecretaris daar hierop ingaan?

De leden van de SP-fractie vragen of de Staatssecretaris kan aangeven welke inschatting wordt gemaakt van het pseudonimiseren waarvan blijkt dat de in de brief aan de Kamer genoemde termijn niet gehaald wordt. Er wordt nu geen nieuwe termijn gegeven wanneer dit gereed moet zijn, maar kan de Staatssecretaris toch een inschatting geven? Hoe houdt de Staatssecretaris de Kamer en de AP op de hoogte van gereedkoming of verdere vertraging?

De leden van de SP-fractie stellen vast dat in antwoord op vraag 12 van de eerder genoemde Kamervragen (Aanhangsel Handelingen II 2017/18, nr. 2345) wordt aangegeven dat op datamining en autorisatie verbetering nodig is. Er wordt gesteld dat hier versneld aan gewerkt wordt. Deze leden willen graag weten wanneer dit gereed is.

Tot slot willen de leden van de SP-fractie aan de Staatssecretaris vragen hoe hij oordeelt over het feit dat de door de AP geconstateerde tekortkomingen die in de eerste onderzoeksperiode bekend, maar «voor lief» genomen werden met als intentie die in de tweede onderzoeksperiode op te lossen, niet opgelost waren in die tweede periode. Is het mogelijk dat er nu privacy-risico's «voor lief» worden genomen met als voornemen deze risico's bij een nieuwe fase op te lossen? Zo ja, hoe voorkomt de Belastingdienst dat dit weer bij een goed voornemen blijft maar niet daadwerkelijk wordt opgelost als er met een nieuwe ICT-omgeving gewerkt gaat worden?

II Reactie van de Staatssecretaris

Inleiding

Uw Kamer heeft een aantal vragen gesteld naar aanleiding van mijn brief van 28 september 2018 welke als bijlagen het afschrift van de brief van de Autoriteit Persoonsgegevens (AP) had over het onderzoek naar de informatiebeveiliging bij de Broedkamer en de afdeling Data & Analytics (D&A) van de Belastingdienst en de reactie van de directeur-generaal Belastingdienst daarop.[4] De Broedkamer is in de loop van 2016 geworden tot de afdeling D&A. De afdeling D&A is vervolgens in 2018 opgegaan in de nieuwe directie Datafundamenten & Analytics (DF&A). In het vervolg van deze beantwoording gebruik ik de afkorting DF&A voor zowel D&A als DF&A.

Alvorens in te gaan op de vragen schets ik voor het overzicht in het kort de gebeurtenissen die geleid hebben tot deze correspondentie. In januari 2017 werd mijn ambtsvoorganger geconfronteerd met de problemen bij de Broedkamer. Op 1 februari 2017 heeft de Belastingdienst een datalek gemeld bij de AP. Om deze redenen besloot hij om onderzoeken in te stellen naar de werkwijze bij de Broedkamer. Op basis van de uitkomsten van de onderzoeken door de Belastingdienst zijn maatregelen doorgevoerd om verantwoord en conform wet- en regelgeving met data-analyse om te gaan.

Voor de AP zijn de ontwikkelingen aanleiding geweest een onderzoek in te stellen naar de beveiliging van de verwerking van persoonsgegevens door de afdeling DF&A van de Belastingdienst.
De AP heeft op 3 juli 2018 aangegeven dat de resultaten van het onderzoek van de Belastingdienst overeenkomen met de resultaten van het onderzoek van de AP.

De beantwoording van de vragen van de vaste commissie van Financiën doe ik daarom aan de hand van vier thema's: de Autoriteit Persoonsgegevens als aanleiding voor de vragen, de Broedkamer en opvolgers als thema voor de door de Belastingdienst getroffen maatregelen, de Algemene Verordening Gegevensbescherming (AVG) voor het verantwoord omgaan met gegevens en Overige vragen voor die onderwerpen die algemeen van aard zijn.

Autoriteit Persoonsgegevens

De leden van de VVD-fractie hebben kennisgenomen van de reactie van de Belastingdienst op het onderzoek van de AP bij de Belastingdienst. Zij hebben nog wel enkele vragen en opmerkingen bij de reactie van de Belastingdienst. Zij merken op dat de AP geen aanleiding ziet om een officieel onderzoeksrapport uit te brengen, terwijl de directeur-generaal Belastingdienst aangeeft dat het voor de Belastingdienst technisch onmogelijk is de privacy van de Nederlanders volledig te waarborgen. Hun vraag is of ik de Kamer op de hoogte kan brengen van de redenen van de AP om geen onderzoeksrapport uit te brengen.

Vooraf merk ik op dat het aan de AP is om te beslissen of zij een rapport uitbrengt. Laat ik daarnaast stellen dat de Belastingdienst zich volledig inspant om zorgvuldig om te gaan met gegevens. Er blijven echter altijd beveiligingsrisico's bestaan als onderdeel van het reguliere operationele proces. Voor geen enkele organisatie is het mogelijk een 100%-beveiliging van gegevens te garanderen.

---

[4] *Kamerstuk* 32 761, nr. 125.

In januari 2017 heeft mijn ambtsvoorganger, meteen na het bekend worden van het potentiële datalek bij de Broedkamer, een melding hiervan gedaan aan de AP. Ook heeft hij diverse onderzoeken laten instellen naar de Broedkamer en DF&A. Op basis van de door de Belastingdienst uitgevoerde onderzoeken zijn er verbetermaatregelen gedefinieerd. Deze maatregelen zijn in mijn brief van 30 juni 2017 met uw Kamer en met de AP gedeeld.[5] Voorts heeft uw Kamer per brief van 2 oktober 2017 alle onderzoeksrapporten van de Belastingdienst die hierop betrekking hebben ontvangen.[6]

Onder meer op basis van de melding van het datalek is de AP begin 2017 een onderzoek gestart naar de informatiebeveiliging van de afdeling DF&A van de Belastingdienst. De AP heeft in juli 2018 geconstateerd dat logging, de controle op de logging en de autorisaties bij de Broedkamer en de opvolgers daarvan, niet op orde waren. De AP constateerde ook dat de resultaten van het onderzoek van de Belastingdienst overeenkwamen met de resultaten van het eigen onderzoek. De AP schrijft: *«Gelet op de toezeggingen over de te nemen verbetermaatregelen die de Staatssecretaris 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. [...] 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.»*[7]

De Belastingdienst heeft de AP bij brief van 19 september 2018 geïnformeerd over de stand van zaken van de toegezegde verbetermaatregelen bij de afdeling DF&A. De leden van de CDA-fractie hebben gevraagd om de reactie van de AP. De AP beoordeelt op dit moment of de verbetermaatregelen die zijn getroffen voldoende zijn en, zo nee, of nader onderzoek nodig is.

Broedkamer en de opvolgers

De leden van de VVD-fractie brengen naar voren dat de AP heeft geconstateerd dat er bij DF&A ten aanzien van de verwerking van persoonsgegevens tekortkomingen bestonden in de informatiebeveiliging. Dit baart de leden zorgen, aangezien dit niet alleen gevolgen heeft voor de privacy, maar ook voor de inning van belastinggeld en de cybersecurity van de Belastingdienst. Zij vragen of ik deze zorgen deel of dat ik van mening ben dat de tekortkomingen met de maatregelen zijn verholpen. Als het laatste het geval is, willen zij graag mijn reactie op de opmerking van de directeur-generaal Belastingdienst dat het technisch onmogelijk is de privacy 100% te beveiligen/garanderen.

De geconstateerde tekortkomingen hadden betrekking op één afdeling. Met de verbetermaatregelen zijn waarborgen geïntroduceerd die ervoor zorgen dat zo zorgvuldig mogelijk wordt omgegaan met gegevens van burgers en bedrijven. Het is echter, zoals gezegd, voor geen enkele organisatie mogelijk om een 100%-beveiliging van gegevens te garanderen. Er blijven altijd beveiligingsrisico's bestaan als onderdeel van het reguliere operationele proces. Beveiliging is in de basis een continu proces van risicomanagement. De Belastingdienst voldoet aan de eisen

[5] *Kamerstuk* 31 066, nr. 367.
[6] *Kamerstuk* 31 066, nr. 379.
[7] *Kamerstuk* 32 761, nr. 125.

op niveau 2, ook bekend als «Departementaal Vertrouwelijk», van de Baseline Informatiebeveiliging rijksoverheid.

De leden van de VVD-fractie vragen zich af op welke technische onmogelijkheden ik doel in mijn reactie aan de AP. Ook vragen zij of technische onmogelijkheden bij het beveiligen van persoonsgegevens kunnen worden opgelost. Ik wil een nadere toelichting geven op die technische onmogelijkheid. Het is niet mogelijk om een bepaalde handeling op dezelfde werkplek, namelijk het kopiëren/verplaatsen van een bestand van de ene werkmap naar een andere werkmap, te loggen. Door middel van de inzet van logging op de handelingen die betrekking hebben op het overige totale werkproces, wordt er voldoende zicht gekregen op waar de gegevens zich bevinden. Logging op deze specifieke handeling is dan ook niet noodzakelijk om alsnog toezicht te houden op de data als geheel.

De leden van de VVD-fractie vragen of er tussen 2 oktober 2017 en oktober 2018 nog casussen bekend zijn waarbij persoonsgegevens per e-mail of andere communicatiemiddelen buiten de Belastingdienst terecht zijn gekomen. Dat is inderdaad het geval. In die periode zijn twee draagbare gegevensdragers met daarop versleutelde gegevens verloren geraakt bij dit dienstonderdeel. Dit is in beide gevallen gemeld als datalek bij de AP. Het feit dat de gegevens versleuteld zijn, maakt dat onbevoegden geen kennis kunnen nemen van de gegevens.

De leden van de VVD-fractie vragen waarom het management van de Belastingdienst heeft gewacht met het implementeren van aanvullende technische verbetermaatregelen terwijl de beveiliging van de gegevens en privacy van vele Nederlanders niet gegarandeerd konden worden. Zij vragen ook of ik op de hoogte was van de tekortkomingen. Als dat het geval was, dan vragen zij zich af of de Kamer niet had moet worden geïnformeerd. De AP stelt in de brief van 3 juli 2018 dat het management van de Belastingdienst op de hoogte was van de tekortkomingen, maar ervoor heeft gekozen om te wachten met de implementatie van aanvullende technische verbetermaatregelen.[8] Deze conclusie heeft betrekking op de periode van 1 januari 2013 tot en met 31 december 2016 (ook bekend als onderzoeksperiode I). In deze periode is de kwestie alleen op directeursniveau besproken. Het management van de Belastingdienst is sindsdien sterk gereorganiseerd en middels de nieuwe Topstructuur is de sturing versterkt conform de COB-aanbevelingen die eerder naar uw Kamer zijn gestuurd.[9]

Na het bekend worden van de problematiek bij de Broedkamer zijn veel verbetermaatregelen doorgevoerd. Ik heb u over de voortgang daarvan geïnformeerd in mijn brief van 30 juni 2017.[10] In dit specifieke geval zijn er mitigerende maatregelen doorgevoerd op het gebied van bewustwording bij DF&A-medewerkers van het op een juiste manier omgaan met persoonsgegevens.

De leden van de VVD-fractie vragen waarom de Belastingdienst heeft gekozen voor een audit door interne auditors met betrekking tot de beveiligings-onderzoeken. Zij vragen of een audit door ADR niet meer op zijn plaats zou zijn geweest.

De Belastingdienst beschikt intern over onafhankelijke auditors. Om te borgen dat het onderzoek kritisch wordt uitgevoerd, is de ADR gevraagd om mee te kijken en een oordeel te geven over dat onderzoek. Op deze

---

[8] *Kamerstuk* 32 761, nr. 125.
[9] *Kamerstuk* 31 066, nr. 330.
[10] *Kamerstuk* 31 066, nr. 367.

wijze is voorzien in het gewenste onafhankelijke oordeel. De conclusie van de ADR was dat het onderzoek door onafhankelijke, gekwalificeerde medewerkers is uitgevoerd conform de richtlijnen van de NOREA. De bevindingen van de ADR heb ik met uw Kamer gedeeld in mijn brief van 2 oktober 2017.[11]

De leden van de VVD-fractie vragen of de Belastingdienst de maatregelen ter verbetering van de privacygegevens ook heeft doorgevoerd bij andere afdelingen dan DF&A. Als dit niet het geval zou zijn, vragen de leden van de VVD-fractie of dan de conclusie terecht is dat die andere afdelingen de persoonsgegevens niet voor 100% kunnen beveiligen.

Beveiliging is een continu proces waarbij geldt dat 100% beveiliging niet gegarandeerd kan worden. De maatregelen zoals toegepast bij DF&A zijn toegepast bij alle medewerkers van DF&A die op één of andere wijze gebruik maken van data-analyse tooling én bij alle medewerkers van de Belastingdienst die gebruik maken van de data-analyse tooling van DF&A. De geconstateerde tekortkomingen waren het gevolg van de inzet van op dat moment voor de Belastingdienst nieuwe technologie waarbij de standaard beveiligingsmaatregelen van de Belastingdienst onvoldoende geïmplementeerd waren. De Belastingdienst gebruikt de Baseline Informatiebeveiliging Rijksdienst als het normenkader voor het inschatten van de risico's en de te nemen maatregelen voor de beveiliging.

De leden van de CDA-fractie merken op dat de brief van de directeur-generaal Belastingdienst een onthutsend beeld schetst. Zij vragen of ik bereid ben om alle toezeggingen over de Broedkamer die zijn gedaan bij het debat over de Belastingdienst op 9 februari 2017, in het algemeen overleg over de Herijking Investeringsagenda Belastingdienst van 25 oktober 2017 en in de brief van 2 oktober 2017 op een rij te zetten en aan te geven of deze zijn opgevolgd.

Hieronder vindt u een overzicht van de toezeggingen en de status van de reeds getroffen beveiligingsmaatregelen. Totdat al deze technische maatregelen zijn geïmplementeerd, blijven procedurele maatregelen van kracht.

Plenair debat 9 februari 2017

Nummer	Toezegging	Status
1	Onderzoek van de AP	De AP beoordeelt of nader onderzoek nodig is
2	Onderzoek gegevensgebruik bij DF&A	Afgerond
3	Onderzoek naar de informatiebeveiliging bij de Broedkamer en voorlopers	Afgerond
4	Extern forensisch onderzoek naar de gevolgde aanbestedingsprocedure voor ondersteuning van de Broedkamer.	Afgerond
5	De Belastingdienst zal bezien op welke wijze het Handboek Beveiliging Belastingdienst is geïmplementeerd in de organisatie, processen en systemen.	Afgerond
6	Uitvoeren in 2017 van een medewerkersonderzoek, waarin naast algemene vragen ook gerichte vragen worden opgenomen over de werkcultuur en managementstijl bij de Belastingdienst.	Afgerond

[11] *Kamerstuk* 31 066, nr. 379.

Algemeen overleg van 25 oktober 2017

Nummer	Toezegging	Status
7	Mogelijkheid om USB te loggen	Zie hierna op p. 11
8	Nagaan of leveranciers datalekken gemeld hebben	De Belastingdienst heeft geen meldingen ontvangen.
9	Overzicht convenanten externe data	Dit overzicht staat op de webpagina van de Belastingdienst.[1]

[1] www.belastingdienst.nl en zoekterm «convenanten»

Brief 2 oktober 2017

Nummer	Toezegging	Status
10	Structurele oplossingen voor continue monitoring	Per 1 oktober 2017 is er sprake van continue monitoring.
11	Pseudonimiseren	Zie hierna op p. 8
12	Datacompartimenteren van de analyseomgeving	compartimentering is laatste kwartaal 2017 gerealiseerd.

De leden van de CDA-fractie vragen om een overzicht van de meldingen van datalekken van de Broedkamer en haar opvolgers in de afgelopen vijf jaar gedaan.

In 2018 zijn twee meldingen van datalekken gedaan aan de AP, beide voor de vermissing van een apparaat met versleutelde gegevens bij de directie DF&A. De meldplicht voor datalekken bestaat sinds 1 januari 2016. Vóór 2016 werden dergelijke incidenten niet als zodanig geregistreerd. Tussen 2016 en 2018 zijn meldingen alleen op het niveau van de Belastingdienst als geheel bijgehouden en niet per directie.
De leden van de SP-fractie hebben enkele vragen over de logging en de daarbij horende triggers binnen DF&A. De leden van de VVD-fractie vragen of de controle op logging geleid heeft tot het afgaan van triggers. De logging en de controle op logging is per 1 oktober 2017 operationeel. Sindsdien zijn enkele triggers afgegaan. Een voorbeeld van een trigger is de volgende situatie: een opvraag levert slechts één uniek gegeven op. Dit kan een teken zijn dat gericht op één specifieke burger gezocht wordt. Maar het kan ook duiden op een fout in de opvraag. Als de trigger af gaat, vindt een gesprek plaats tussen de betrokken medewerker en zijn leidinggevende. Gebleken is dat in al deze gevallen sprake was van een toegestane verwerking. Op termijn wordt het geheel van triggers geëvalueerd.
De leden van de CDA-fractie vragen ook of er sprake is van algemene logging binnen de applicaties van de Broedkamer, hoe het zit met het loggen van de export van data vanuit de brongegevens en of er ooit aanwijzingen gevonden zijn dat er data buiten de Belastingdienst is geëxporteerd.
De logging is operationeel sinds 1 oktober 2017. De directie DF&A zet logging in op de risicovolle delen van de werkprocessen van DF&A. Er is geen sprake van algemene logging. Onder «export van data» wordt in dit verband overigens verstaan het overzetten van data van de ene beveiligde omgeving binnen de Belastingdienst naar de andere beveiligde omgeving van de Belastingdienst. Op basis van de per 1 oktober 2017 operationele logging, heb ik geen aanwijzingen gevonden dat er data buiten de Belastingdienst is geëxporteerd.
De leden van CDA-fractie vragen ook of individuele analisten een data «check out» mogen doen naar een lokale omgeving. Individuele analisten mogen een «check out» doen naar een lokale omgeving. De handeling wordt gelogd en er is een procedure omheen beschreven voor een zorgvuldige omgang met de gegevens.

De leden van de SP-fractie vragen of het mogelijk is dat er op papier goede processen zijn beschreven, maar dat die in de praktijk niet opgevolgd worden.

Onderdeel van het procesontwerp zijn interne controleprogramma's. Deze interne controleprogramma's zorgen ervoor dat eventuele tekortkomingen ontdekt kunnen worden en dat maatregelen gedefinieerd worden om deze tekortkomingen te verhelpen. Hierdoor worden processen constant geëvalueerd.

De leden van de SP-fractie vragen of de Staatssecretaris kan aangeven welke inschatting wordt gemaakt van het pseudonimiseren. Zij vragen of ik kan inschatten wanneer dit gereed kan zijn. De leden van de CDA-fractie vragen naar het tijdpad voor pseudonimisering.

In zijn brief van 19 september 2018 aan de AP heeft de directeur-generaal Belastingdienst aangegeven dat de voorbereidingen nodig voor implementatie substantieel en complex zijn en dat in het plan van aanpak geen termijnen gegeven kunnen worden. Uw Kamer heeft op 28 september 2018 een afschrift van deze brief ontvangen.[12] Ten aanzien van de implementatie kunnen er nog geen exacte termijnen gegeven worden vanwege onder andere de massaliteit en complexiteit van de benodigde aanpassingen in de opzet van de gegevensbestanden en de schaarste aan kennis in de markt. Het betreft hier immers miljoenen bestanden in de verschillende systemen van de Belastingdienst. De verwachting is dat nieuwe systemen sneller aangesloten kunnen worden dan bestaande, omdat bij nieuwe systemen in het ontwerp al rekening gehouden moet worden met de principes van *privacy by design*. In de reguliere rapportages aan uw Kamer zal ik u op de hoogte houden over de voortgang van het pseudonimiseren.

Algemene Verordening Gegevensbescherming

De leden van de VVD-fractie vragen of ik de Kamer kan informeren over de voortgang met betrekking tot het voldoen aan de Algemene verordening gegevensbescherming (AVG). Zij vragen of de gehele Belastingdienst, zoals ik eerder heb toegezegd, eind 2018 zal voldoen aan een AVG-compliant situatie. De leden van de SP-fractie merken op dat zij het zorgelijk vinden dat zo een belangrijke overheidsdienst als de Belastingdienst maar liefst een jaar de tijd nodig heeft om aan de AVG te voldoen. Zij vragen of ik kan aangeven of dit nog steeds als haalbare termijn wordt gezien of is er inmiddels vertraging opgelopen en zo ja, op welke onderdelen precies.

De Belastingdienst is een grote gegevensverwerkende organisatie met miljoenen dossiers, waarbij het uitvoeren van de maatregelen veel werk is. Het belang van privacy staat hierbij hoog in het vaandel. Een aantal deadlines staat echter onder druk en ik heb aan de Belastingdienst gevraagd om hierop strak te sturen. Hierbij gaat het met name om het schonen en archiveren van gegevens en de actualiteit van autorisaties. Daarbij gaat het om grote hoeveelheden documenten waar met zorgvuldigheid mee om moet worden gegaan. In de antwoorden van 6 juni 2018 is aan uw Kamer medegedeeld dat de Belastingdienst streeft naar een volledige implementatie binnen een jaar, gerekend vanaf 25 mei 2018.[13]

---

[12] *Kamerstuk* 32 761, nr. 125.
[13] *Aanhangsel Handelingen II* 2017/18, nr. 2345.

De AP verwijst naar een aantal tekortkomingen in de naleving van de AVG. De leden van de VVD-fractie vragen of ik de Kamer per tekortkoming kan informeren over de genomen maatregelen om deze tekortkomingen te verhelpen. De AP heeft met de brief van 3 juli 2018 de Belastingdienst geïnformeerd over de resultaten van het onderzoek en over de daarbij geconstateerde overtredingen van de privacyregelgeving. De geconstateerde tekortkomingen betreffen logging, controle op de logging en autorisaties. Het betrof tekortkomingen die de Belastingdienst zelf ook in 2017 geconstateerd heeft. De te treffen verbetermaatregelen horende bij de genoemde tekortkomingen zijn dan ook in 2017 in gang gezet en daarover heb ik uw Kamer geïnformeerd met de Kamerbrief van 30 juni 2017[14] en het algemeen overleg van 14 december 2017.[15]

De leden van de VVD-fractie merken op dat de Belastingdienst privacygegevens van Nederlanders niet 100% kan beveiligen. Zij vragen of de Belastingdienst wel 100% inzicht heeft in de beschikbare data.

De Belastingdienst heeft 100% inzicht in de beschikbare data.

De leden van de CDA-fractie zijn verbaasd dat DF&A nu als AVG-compliant wordt beschouwd. Graag ontvangen deze leden hiervan een auditrapport.

In de eerder genoemde brief van 19 september 2018 aan de AP schrijft de directeur-generaal Belastingdienst dat met het treffen van de maatregelen op basis van de onderzoeken en het realiseren van de basispositie AVG de directie DF&A compliant is met de AVG.[16] Er loopt nu een auditonderzoek om dit ook feitelijk vast te stellen. De resultaten zal ik met uw Kamer delen.

De leden van de CDA-fractie vragen of de Belastingdienst bereid is om aan te geven waar een burger of bedrijf kan vragen welke data DF&A over hem/haar heeft en hoe hij/zij daar inzage in kan krijgen en hoeveel burgers van dat recht gebruik hebben gemaakt.

Op de website van de Belastingdienst is de procedure beschreven hoe een burger gebruik kan maken van zijn recht.[17] Daarbij merk ik op dat daarbij niet gevraagd kan worden naar specifieke organisatieonderdelen. Het verzoek betreft de Belastingdienst als geheel. Sinds 25 mei 2018 zijn bij de Belastingdienst zestig verzoeken binnengekomen van burgers die inzage gevraagd hebben naar hun fiscale gegevens.[18]

De leden van de CDA-fractie vernemen graag welke vorderingen de Belastingdienst in zijn algemeenheid heeft geboekt voor het bereiken van AVG compliantie.

Privacy en beveiliging hebben hoge prioriteit. Daarbij is het toezicht op de naleving van de AVG een continu proces. Ten behoeve van de dagelijkse uitvoering heeft de Belastingdienst technische en organisatorische maatregelen getroffen. Het gaat hierbij bijvoorbeeld om het uitvoeren van gegevensbeschermingseffectbeoordelingen en het afsluiten van verwerkersovereenkomsten. Ik heb uw Kamer daarover geïnformeerd op 6 juni

---

[14] *Kamerstuk* 31 066, nr. 367.
[15] *Kamerstuk* 31 066, nr. 394.
[16] *Kamerstuk* 32 761, nr. 125.
[17] https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/niet_in_enig_menu/prive/privacy.
[18] Stand van zaken per medio december 2018.

2018 bij de beantwoording van Kamervragen over de AVG en de Belastingdienst.[19]

De leden van de SP-fractie stellen vast dat in antwoord op vraag 12 van de eerder genoemde Kamervragen wordt aangegeven dat op datamining en autorisatie verbetering nodig is.[20] Er wordt gesteld dat hier versneld aan gewerkt wordt. Deze leden willen graag weten wanneer dit gereed is.

Ik heb in het antwoord op vraag 12 aangegeven dat verbeteringen nodig zijn in een aantal toezicht- en bedrijfsvoeringsapplicaties op het gebied van dataminimalisatie en autorisatie. Dataminimalisatie houdt in dat bij het verzamelen en verwerken van persoonsgegevens niet méér gegevens mogen worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken. De maatregelen voor dataminimalisatie en het in lijn brengen van de autorisaties lopen mee in het traject van maatregelen die de Belastingdienst uitvoert en een streefdatum kennen van 25 mei 2019.

De leden van de SP-fractie vragen ook hoe ik oordeel over het feit dat de door de AP geconstateerde tekortkomingen die in de eerste onderzoeksperiode bekend, maar «voor lief» genomen werden met als intentie die in de tweede onderzoeksperiode op te lossen, niet opgelost waren in die tweede periode. Daarbij vragen zij hoe de Belastingdienst bij een volgende nieuwe ICT-omgeving niet weer de privacy-risico's in fasen wegneem.

Mijn beeld is dat uit de onderzoeken van mijn ambtsvoorganger en uit die van de AP blijkt dat beveiliging lager op de prioriteitenlijst van het toenmalig management stond dan functionaliteit van de analyse-omgeving. De inwerkingtreding van de AVG maakt dat *privacy by design* de nieuwe standaard is. Het instrument van de gegevensbeschermingseffectbeoordeling zoals dat nu verplicht te gebruiken is voor risicovolle verwerkingen helpt de Belastingdienst bij het vroegtijdig detecteren van de risico's en maakt dat er op voorhand mitigerende maatregelen meegenomen worden in het ontwerp van een nieuwe ICT-omgeving.

Overige vragen

De leden van de CDA-fractie vragen hoe de «werkplek van een medewerker» is vormgegeven.

De digitale werkplek van iedere medewerker van de Belastingdienst bestaat onder andere uit een draagbare computer uitgerust met een standaard besturingssysteem en aanvullende beveiligingsmaatregelen als versleuteling van de gegevens op de harde schijf en uitgeschakelde USB-poorten waarbij alleen toegang gekregen kan worden tot de werkplek na het ingeven van de gebruikersnaam en bijbehorend wachtwoord.

Daarnaast willen zij graag weten waarom het niet technisch onmogelijk wordt gemaakt om data op een USB-stick te zetten en of er logging is in dit verband. Het is reeds technisch onmogelijk gemaakt om zonder toestemming (autorisatie) gebruik te maken van een USB-poort. Bij DF&A worden geen autorisaties verleend voor het gebruik van de USB-poort voor het lezen of schrijven van bestanden op een verwisselbaar medium.

---

[19] *A anhangsel Handelingen* II 2017/18, nr. 2345.
[20] *Aanhangsel Handelingen* II 2017/18, nr. 2345.

De leden van de VVD-fractie vragen wat de Belastingdienst doet bij overtreding van de procedures omtrent het schrijven van data op een USB-stick en wie toegang heeft tot het register.

Een medewerker kan geautoriseerd worden voor het mogen lezen en schrijven van gegevens via de USB-poort. Als een medewerker niet geautoriseerd is, is de USB-poort niet actief. Het register waarnaar verwezen wordt, is beschikbaar voor het management van een kantoor en is een afschrift van het systeem waarmee de daadwerkelijke autorisatie geregeld wordt. Hierin wordt de historie van de autorisaties vastgelegd. Bij misbruik geldt het reguliere sanctieproces.

De leden van de VVD-fractie vragen hoeveel trainingen en bewustwordingssessies de medewerkers van de Belastingdienst jaarlijks volgen en wat daarbij aan de orde komt.

Op het gebied van bewustwording en kennis zijn onder andere e-learning modules verplicht gesteld, worden nieuwe medewerkers tijdens de inwerkperiode gewezen op de plichten en zijn de managers getraind om binnen de eigen teams de toepassing van de AVG te bespreken. Ik heb uw Kamer daarover ook geïnformeerd op 6 juni 2018 bij de beantwoording van de Kamervragen over de AVG en de Belastingdienst.[21]

De leden van de SP-fractie maken zich zorgen over het feit dat niet wordt bijgehouden welke gegevens door medewerkers worden opgevraagd. Deze leden vragen mij wanneer de Belastingdienst kan garanderen dat gevoelige persoonsgegevens niet buiten de systemen belanden.

Hoewel het belang van privacy hoog in het vaandel staat, kan ik u die garantie niet geven. 100% Beveiliging van gegevens bestaat helaas niet. De gegevens zijn beschermd met maatregelen op het niveau «Departementaal Vertrouwelijk».

Dezelfde leden vinden het terecht dat bij gebrek aan het kunnen aanpassen van autorisaties aan bewustwording wordt gedaan, maar zij maken zich zorgen dat via mobiele apparaten nog altijd bijlagen kunnen worden opgeslagen. Zij vragen naar de sancties.

Tijdens het algemeen overleg van 6 december 2018 heb ik uw Kamer een brief toegezegd over de sancties. Die brief is ondertussen verzonden.[22] Het sanctieregime is gericht op het voorkomen van bewust fout gedrag en dat gedrag, als het dan toch gebeurt, te bestraffen. Via mobiele apparaten kunnen, net zoals vanaf de portable computer, bijlagen verzonden worden bij een e-mail. Voor medewerkers die gebruik maken van data-analyse tooling is het niet mogelijk om externe e-mailadressen van buiten de Belastingdienst hierbij te gebruiken.

Als het gaat om de autorisaties en toegangsrechten vragen de leden van de SP-fractie of het mogelijk is dat een medewerker die de Belastingdienst verlaat toch nog maximaal 30 dagen toegang houdt, omdat eens per maand een volledige check wordt uitgevoerd. Zij zijn van oordeel dat de autorisatie dan direct zou moeten worden ingetrokken.

Bij uitdiensttreding moet de medewerker de digitale werkplek, toegangspas en eventuele mobiele apparaten uiterlijk op de laatste werkdag inleveren bij de teammanager. Daarnaast wordt op basis van het signaal uit P-Direct dat het dienstverband beëindigd is, het account

[21] *Aanhangsel Handelingen* II 2017/18, nr. 2345.
[22] *Kamerstuk* 31 066, nr. 448.

automatisch geblokkeerd. Zonder digitale werkplek of mobiel apparaat is geen toegang meer te krijgen tot de gegevens en applicaties van de Belastingdienst. Feitelijk wordt daarmee voldaan aan de wens van deze vragenstellers.