Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

696

Vragen van de leden **Lodders** en **Middendorp** (beiden VVD) aan de Staatssecretarissen van Financiën en van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Beveiliging data fiscus ondermaats»* (ingezonden 23 oktober 2018).

Antwoord van Staatssecretaris **Snel** (Financiën), mede namens de Minister en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 19 november 2018).

Vraag 1
Bent u bekend met het bericht «Beveiliging data fiscus ondermaats»?[1]

Antwoord 1
Ja.

Vraag 2
Welke technische onmogelijkheden om persoonsgegevens goed te beveiligen bedoelt de Belastingdienst precies? Kunt u specifieker zijn over wat er wel en niet mogelijk is?

Antwoord 2
Op 28 september heb ik een afschrift van een brief aan de AP aan uw Kamer gestuurd, waarin wordt ingegaan op de gerealiseerde verbetermaatregelen bij de afdeling Datafundamenten en Analytics (DF&A) van de Belastingdienst. In die brief is aangegeven dat «vanuit de dataomgeving bij afdeling DF&A, waar wel een exportfunctie aanwezig is, technische logging niet mogelijk [is] noch het aanpassen van autorisaties». Op basis van deze zin wordt in het artikel de indruk gewekt dat de gegevensbeveiliging bij de Belastingdienst in den brede niet op orde is. Dat is niet het geval.
De situatie is dat het niet mogelijk is om ieder gebruik van gegevens te loggen als de te analyseren gegevens eenmaal uit de centrale dataomgeving zijn gehaald en in de digitale werkomgeving (PC of laptop) van de medewerker van DF&A zijn geplaatst. Dat komt omdat in de digitale werkomgeving van de medewerker ook standaardapplicaties worden gebruikt die geen logmogelijkheid kennen. Daarom zijn technische- en organisatorische

[1] Trouw, 12 oktober 2018, https://www.trouw.nl/home/belastingdienst-het-is-technisch-onmogelijk-persoonsgegevens-goed-te-beveiligen~a8648a26/

ah-tk-20182019-696
ISSN 0921 - 7398
's-Gravenhage 2018

maatregelen getroffen in het werkproces, waarmee het risico van een datalek wordt geminimaliseerd (zie het antwoord op vraag 7). Handelingen met gegevens in de centrale dataomgeving van DF&A worden wel gelogd en gemonitord.

Vraag 3
Wordt met «technisch onmogelijk» bedoelt de huidige IT-security-middelen die nu ter beschikking zijn, of meer in algemene zin?

Antwoord 3
Met technisch onmogelijk is inderdaad bedoeld dat dit niet mogelijk is in de huidige digitale werkomgeving van de medewerkers. Dit zal worden opgelost met invoering van de zogenoemde Analytical Data Perimeter (ADP). Dit is een technisch volledig afgesloten digitale werkomgeving waar enkel vooraf gedefinieerde, gecontroleerde en geaccordeerde dataroutes mogelijk zijn, die steeds gelogd en gemonitord worden. De ADP wordt op dit moment gebouwd en zal in de loop van 2019 beschikbaar zijn.

Vraag 4
Zou het met meer kennis en kunde en/of een betere algemene ICT-architectuur bij de overheid (denk aan de door Binnenlandse Zaken en Koninkrijksrelaties geleverde DigiD-architectuur) wel mogelijk zijn om persoonsgegevens bij de Belastingdienst te beveiligen? Zo nee, waarom niet?

Antwoord 4
Er is geen sprake van dat persoonsgegevens bij de Belastingdienst niet beveiligd zijn. Zoals in de beantwoording onder vraag 2 is aangegeven, betreft het in het geval van de Belastingdienst de beveiligingsmaatregel logging op één onderdeel van het werkproces bij DF&A. Maatregelen om een adequate beveiliging van dat specifieke onderdeel te borgen, zijn getroffen (zie het antwoord op vraag 7). Verder is de informatiebeveiliging (inclusief het toegangsbeheer) bij de Belastingdienst gebaseerd op rijksbrede kaders zoals de Baseline informatiebeveiliging Rijk (BIR).
De overheid blijft uiteraard investeren in kennis en kunde en in het leveren van een goede architectuur. Toepassing van DigiD of de DigiD-architectuur biedt in dezen geen oplossing, aangezien DigiD specifiek is ontwikkeld voor authenticatie (het verifiëren van de identiteit) van natuurlijke personen die inloggen bij digitale loketten zoals MijnBelastingdienst of MijnOverheid. Het werkproces van de afdeling DF&A betreft analyse van gegevens in de interne systemen van de Belastingdienst.

Vraag 5
Klopt de berichtgeving dat de Belastingdienst geen inzicht heeft in waar welke data zich bevindt in de systemen? Deelt u de mening dat dit een zorgelijke constatering is, aangezien die namelijk niet alleen gevolgen heeft voor de privacy, maar ook voor de business in het algemeen alsook de cybersecurity in het algemeen? Hoe kan de Belastingdienst de data voor 100% beveiligen als niet alles kenbaar of zichtbaar is?

Antwoord 5
Het is mij niet duidelijk op welke berichtgeving in deze vraag wordt gedoeld. Het is niet zo dat de Belastingdienst geen inzicht heeft in de plaatsen waar (persoons)gegevens zich bevinden in de ICT-systemen, en welke gegevens dat zijn.

Vraag 6
Deelt u de mening dat het opslaan van geselecteerde persoonsgegevens in één heldere en unieke bron het probleem van het gebrek aan overzicht bij de Belastingdienst waar persoonsgegevens zich bevinden zou oplossen? Zo ja, wat wordt er bij de Belastingdienst gedaan om dit voor elkaar te krijgen? Zo nee, waarom niet? Krijgen medewerkers van de Belastingdienst en andere overheidsinstellingen die werken met persoonsdata hier speciale trainingen voor? Zo ja, hoe zien deze trainingen eruit? Zo nee, waarom niet?

Antwoord 6
Zoals aangegeven in het antwoord op vraag 5 is geen sprake van het ontbreken van inzicht waar persoonsgegevens zich bevinden.
De ICT-systemen bij Belastingdienst zijn ingericht per belastingmiddel en er zijn afzonderlijke systemen voor toeslagen en douane. Dat is voor een goede uitvoering van de verschillende taken ook noodzakelijk. Wel wordt er naar gestreefd gegevens voor analysedoeleinden (zoals de afdeling DF&A die verricht) op te slaan in één bron. Daarbij worden specifieke maatregelen genomen (zie ook vraag 7) om de informatieveiligheid te verzekeren; hierop wordt een audit uitgevoerd.
Alle medewerkers van de Belastingdienst zijn verplicht de training iBewustzijn Overheid te volgen, die onder meer modules bevat over verantwoord omgaan met persoonsgegevens en met digitale middelen die het werk ondersteunen, en over het veilig houden van de fysieke werkomgeving. Vanaf het voorjaar van 2018 is hier een specifieke AVG-module aan toegevoegd. De certificaten die worden behaald bij het doorlopen van de training worden toegevoegd aan het personeelsdossier.

Vraag 7
Wat heeft de Belastingdienst veranderd aan de beveiliging van persoonsgegevens sinds de uitzending van Zembla begin 2017? Heeft deze verandering alleen plaatsgevonden bij de afdeling Data & Analytics of ook bij andere afdelingen? Zo ja, welke afdelingen en wat is er precies veranderd? Zo nee, waarom niet?

Antwoord 7
Sinds de uitzending van Zembla zijn bij het dienstonderdeel DF&A de volgende maatregelen getroffen:
- De gegevens zijn gecompartimenteerd, zodat medewerkers alleen de gegevens te zien krijgen die zij nodig hebben voor hun werk.
- Toegang tot de datacompartimenten is strikt geregeld via autorisaties.
- De autorisaties worden maandelijks volledig beoordeeld op actualiteit en geldigheid.
- Iedere gegevensverwerking in de dataomgeving werd al gelogd en wordt nu actief gemonitord; er wordt gecontroleerd of voldaan is aan vooraf gedefinieerde beveiligingsregels (bijvoorbeeld: er mag niet gezocht worden op een specifieke persoon). Zo niet dan volgt een signaal naar de medewerker en zijn leidinggevende. Als blijkt dat van een onrechtmatigheid sprake is, wordt het reguliere proces voor integriteitsschendingen gevolgd.
- In de beveiligde werkomgeving van de medewerker met datatoegang is extern mailverkeer niet meer mogelijk. Het via een mobile device (die zijn voorzien van een wachtwoord en afgedwongen beveiligingsmaatregelen) opslaan en versturen van bijlagen is alleen mogelijk door middel van doelbewuste handelingen. In de trainingen en bewustwordingssessies van alle medewerkers wordt het verrichten van deze handelingen bestempeld als een bewuste en kwaadwillende actie, die kan leiden tot sancties.
- Gebruik van internet is alleen mogelijk naar goedgekeurde websites; export van gegevens naar het internet is afgesloten.
- De medewerkers die geautoriseerd zijn voor het werken met data beschikken niet over USB-ontheffingen en kunnen deze ook niet verkrijgen. Alleen beheerders kunnen een USB-ontheffing aanvragen van enkele uren (dit is het afgelopen jaar niet gebeurd).
- Alle bevoegdheden voor gebruik van file transfer (FTP) naar buiten zijn ingetrokken.

Verder zijn bij de Belastingdienst met behulp van risico- en issueanalyses op verwerkingen van persoonsgegevens verbetermaatregelen geformuleerd. Op het gebied van informatiebeveiliging betreffen deze verbetermaatregelen met name de actualisering en het beheer van autorisaties van medewerkers voor het gebruik van gegevens.

Vraag 8
Zijn er naast de Belastingdienst en het Uitvoeringsinstituut Werknemersverzekeringen nog meer overheidsinstellingen die problemen ervaren met de beveiliging van persoonsdata? Hoe bent u voornemens persoonsgegevens in de toekomst overheidsbreed wel optimaal te beveiligen? Wat wordt er in

samenwerking met andere departementen door u gedaan om dit te implementeren?

Antwoord 8
Voorop staat dat overheidsorganisaties zelf verantwoordelijk zijn en blijven voor de beveiliging van hun persoonsgegevens. Nog niet alle organisaties hebben dit volledig op orde, maar er wordt hard aan gewerkt en dit onderwerp heeft overheidsbreed hoge prioriteit. De openbare onderzoekrapportages van de Autoriteit Persoonsgegevens[2] geven een goede indicatie van het type problemen dat overheidsinstellingen op dit terrein ervaren. In samenwerking met andere ministeries worden de nodige initiatieven ontplooid om duurzame naleving van de AVG op dit vlak binnen het Rijk te bevorderen. Het Ministerie van BZK faciliteert dit onder meer door de introductie van een nieuwe rol, de Privacy Adviseur Rijksbrede Kaders & Voorzieningen (PAR) en een bijbehorende procedure voor rijksbrede projecten. Met deze aanpak wordt centraal, in afstemming met alle ministeries, één privacy-advies opgesteld voor Rijksbrede kaders en voorzieningen. In de update van de Strategische I-agenda voor de Rijksdienst, die uw Kamer na het Kerstreces ontvangt, zal de Minister van BZK nader ingaan op de verdere uitwerking van deze en andere privacy-versterkende maatregelen voor de sector Rijk.

Vraag 9
Wanneer verwacht u dat de Belastingdienst kan voldoen aan de striktere regels omtrent de Algemene Verordening Gegevensbescherming?

Antwoord 9
Ik verwacht dat de Belastingdienst per mei 2019 de implementatie van de verbetermaatregelen afgerond zal hebben en in lijn zal zijn met de AVG. Bij de afdeling DF&A is dit, zoals ook aangegeven in de brief aan de AP, eind mei 2018 al gerealiseerd. Naleving van de AVG is echter een continu proces dat structureel aandacht en maatregelen vraagt en nooit «af» is.

Vraag 10
Wanneer verwacht u dat technische onmogelijkheden bij het beveiligen van persoonsgegevens zijn opgelost? Welke stappen moeten naast bovengenoemde nog gezet worden?

Antwoord 10
Zoals aangegeven in het antwoord op vraag 3 zal het in gebruik nemen van de ADP de technische onmogelijkheid van met logging in de werkomgeving van de medewerkers van DF&A oplossen.
Voor de andere onderdelen van de Belastingdienst geldt dat het nemen van informatiebeveiligingsmaatregelen, afgestemd op aard en omvang van de gegevensverwerkingen, een reguliere activiteit is. Specifieke stappen hoeven daarvoor niet te worden gezet.

Vraag 11
Kunt u de Kamer zo snel mogelijk informeren over mogelijke vervolgstappen van de Autoriteit Persoonsgegevens? Zo nee, waarom niet?

Antwoord 11
Ik zal uw Kamer informeren over vervolgstappen van de Autoriteit Persoonsgegevens zodra ik daarover door de Autoriteit word geïnformeerd.

Vraag 12
Wilt u alle vragen één voor één beantwoorden?

Antwoord 12
Ja.

[2] Beschikbaar op de website www.autoriteitpersoonsgegevens.nl.