Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

# 31 066 Belastingdienst

**Nr. 340** **BRIEF VAN DE STAATSSECRETARIS VAN FINANCIËN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 februari 2017

Op 1 februari jl. was er een uitzending van het televisieprogramma Zembla waarin de Belastingdienst en in het bijzonder de afdeling Data & Analytics (D&A) centraal stond. Zembla meldde dat de informatiebeveiliging niet op orde zou zijn. In de uitzending kwam bovendien aan de orde dat sprake zou zijn van niet integer handelen bij een aanbesteding, van het uiten van onwaarheden over verwachte opbrengsten van de aanpak van D&A en van een onbehoorlijke managementstijl.

Tijdens het debat van 2 februari jl. heeft uw Kamer diverse vragen gesteld die zijn opgenomen in de op vrijdag 3 februari aan mij toegestuurde schriftelijke vragen. Alvorens in te gaan op de gestelde vragen wil ik benadrukken dat de in de uitzending gedane aantijgingen ernstig zijn. Hoewel op dit moment niet vaststaat dat regels zouden zijn overtreden, moeten signalen als deze uiterst serieus worden genomen. De signalen worden dan ook onderzocht door de Autoriteit Persoonsgegevens. In afwachting van de uitkomsten daarvan neem ik extra maatregelen om te zorgen dat risico's maximaal worden uitgesloten.
Ook moet de Belastingdienst in zijn aanbestedingen elke schijn van belangenverstrengeling vermijden. Signalen over niet integer gedrag worden dan ook serieus genomen en onderzocht.

Het in mijn ogen opnieuw meest pijnlijke punt is dat medewerkers zich blijkbaar geroepen hebben gevoeld hun zorgen anoniem te melden buiten de Belastingdienst in plaats van daarbinnen. Dit is onaanvaardbaar voor een organisatie die voor zijn verbeteringen vooral afhankelijk is van de eigen medewerkers. De medewerkers die hun zorgen hebben geuit via Zembla, roep ik dan ook op hun informatie – zo nodig anoniem – te verstrekken aan het onafhankelijke meldpunt dat op korte termijn zal worden ingericht. Zoals ik heb aangegeven in de brief bij de continuïteitsrapportage d.d. 27 januari jongstleden (Kamerstuk 31 066, nr. 331), zal contact worden opgenomen met het Huis voor Klokkenluiders over de meest geschikte vorm voor dit meldpunt. Op die wijze kunnen de door medewerkers afgegeven signalen meer gericht worden onderzocht.

kst-31066-340
ISSN 0921 - 7371
's-Gravenhage 2017

Een methodiek om de verwachte potentiële correctieopbrengsten van de Investeringsagenda te ramen is, zoals ik ook in mijn brief van 11 oktober 2016 heb aangegeven,[1] in ontwikkeling. Ik zal de president van de Algemene Rekenkamer (ARK) verzoeken deze te toetsen.

In deze brief ga ik in op de vier onderwerpen die in de uitzending van Zembla aan de orde waren. In een bijlage bij deze brief zijn de antwoorden op de gestelde vragen opgenomen.

## 1. Informatiebeveiliging

De informatiebeveiliging bij de Belastingdienst in het algemeen en bij D&A in het bijzonder moet op orde zijn. De ICT-infrastructuur van de Belastingdienst, inclusief D&A, voldoet aan het reguliere informatiebeveiligingsbeleid op grond van het Handboek Beveiliging Belastingdienst (HBB). Gelet op de aard van het document volsta ik hier met het noemen op hoofdlijnen van enkele eisen uit het HBB die ook voor de context van D&A relevant zijn. Ik stuur het HBB ter vertrouwelijke inzage mee met deze brief[2].

*ICT- beveiliging*
- Toegangsbeveiliging voor systemen door middel van gebruikersnaam en wachtwoord.
- Autorisatie voor toegang tot gegevens op basis van rol, regelmatige actualisering.
- Logging en monitoring van systemen op gebruik, zoals op toegang verkrijgen, bewerkingen, gebruik van speciale bevoegdheden, aangebrachte wijzigingen.
- Transport van gegevens via beveiligde dragers (bv. via encyptie).

*Fysieke beveiliging*
- Scheiding tussen openbare ruimtes (balies ed.) en kantoorruimtes, conform de rijksbrede normenkaders. Logging van toegang tot gebouwen.
- Extra fysieke beveiliging van datacenters.
- Clear desk en clear screen beleid, automatische vergrendeling van computers en laptops bij niet-gebruik.

Hieruit volgt dat medewerkers (intern of extern) bij de Belastingdienst geen onbelemmerde toegang hebben tot alle gegevens, maar dat de toegang en de wijze van gebruik van die gegevens beperkt is tot wat voor de uitoefening van hun functie noodzakelijk is. Voor medewerkers van D&A geldt op grond van de eisen dat zij belastinggegevens van belastingplichtigen alleen kunnen zien en hier analyses op kunnen doen, maar dat zij deze niet kunnen wijzigen.

Voor de toepassing van het algemene beveiligingsbeleid van de Belastingdienst bij D&A is vanaf het moment van oprichting van D&A, in februari 2016, systematisch aandacht. De periode daarvoor, toen de activiteiten nog plaatsvonden in het programma Broedkamer en de opstart daarvan, laat ik nader onderzoeken. Om ook overigens iedere twijfel uit te sluiten, laat ik ook een breed onderzoek uitvoeren naar de toepassing van het beveiligingsbeleid bij de Belastingdienst.

In de uitzending van Zembla is gerefereerd aan een rapport van de Auditdienst Rijk over onder meer de (informatie)beveiliging bij D&A.

---

[1] Kamerstuk 31 066, nr. 304.
[2] Ter vertrouwelijke inzage gelegd, alleen voor de leden, bij het Centraal Informatiepunt Tweede Kamer.

Hieronder schets ik de context van dit rapport en de bevindingen daarin. Bij de oprichting van D&A begin 2016 heeft de Belastingdienst aan de ADR gevraagd om mee te kijken met en te adviseren over aanvullende beheersmaatregelen voor de gehele bedrijfsvoering van het op te richten D&A, inclusief (informatie)beveiliging. Daarbij heeft D&A onder andere aangegeven welke gedachten men had over extra beveiligingsmaatregelen, bovenop wat ingevolge het HBB al voor de Belastingdienst geldt, en de ADR gevraagd daarop te reageren.
De ADR heeft daarover op 10 maart 2016 een interimrapport uitgebracht. Dit is het rapport waaraan in de uitzending van Zembla wordt gerefereerd. Dit rapport is toegezonden aan Uw Kamer als bijlage bij mijn brief van op 28 oktober 2016.[3] De ADR-constateerde met betrekking tot de aanvullende beveiligingsvoornemens van D&A:

*«3.7 Beveiliging*
*Vanwege de hoge mate van gevoeligheid van de data waarmee binnen D&A wordt gewerkt, heeft D&A aandacht voor de vertrouwelijkheid van de data. Om het gewenste beveiligingsniveau te bereiken, wordt bijvoorbeeld spaarzaam omgegaan met het verlenen van een USB-ontheffing aan medewerkers. Een privacy officer is recent aangesteld, zijn werkzaamheden zijn nog niet uitgekristalliseerd.*

*In opdracht van de RvB gaat D&A samen met B/CA een visie op omgang met data opstellen. Een data management framework zal op basis van deze visie worden vervaardigd. Dit framework wordt naar verwachting eind Q1 2016 opgeleverd. Voor beperking van fysieke toegang (zie 3.6 Huisvesting) en nadere inperking van de logische toegangsbeveiliging om data voor medewerkers af te schermen, zijn gedachten aanwezig zoals toegangspasjes om op de afdeling te komen, logging en monitoring. Deze maatregelen zijn nog niet geëffectueerd.»*

Alleen de laatste alinea werd geciteerd in het programma Zembla. Anders dan door Zembla op basis hiervan wordt gesuggereerd, betekent dit niet dat er geen logging en monitoring plaatsvond bij D&A. Er werd en wordt minimaal gelogd wie wanneer iets doet, wat iemand doet en welke directories, bestanden en databasetabellen worden gebruikt. De bevinding van de ADR betrof de aanscherping van deze logging en monitoring. Desalniettemin heb ik opdracht gegeven om de beschikbare loggegevens (zowel uit de periode van de Broedkamer als van D&A) te onderzoeken, zodat kan worden vastgesteld of getracht is daadwerkelijk gegevens van belastingplichtigen buiten de Belastingdienst te brengen. Tevens heb ik opdracht gegeven het gegevensgebruik van de Broedkamer en zijn voorgangers nader te onderzoeken.

Logischerwijs waren de ideeën over aanvullende beveiligingsmaatregelen nog niet geëffectueerd, omdat D&A zich in de fase van oprichting bevond. Snel na de oprichting is gestart met het formuleren en realiseren van de aanvullende beschermende maatregelen, naast de standaardmaatregelen van het HBB. Deze maatregelen zijn opgenomen in een bijlage bij deze brief.

Ik zal de Minister van BZK vragen om in de bijlage genoemde aanwijzing als bijzonder werkgebied van de afdeling D&A zo snel mogelijk te effectueren. Daarnaast zullen bij D&A extra bijeenkomsten worden georganiseerd om het belang van zorgvuldige omgang met gegevens en de daarvoor geldende regels nogmaals onder de aandacht te brengen bij de medewerkers en zal de privacyfunctionaris voor dit aspect worden

[3] Kamerstuk 31 066, nr. 315, bijlagen.

ingezet bij het selecteren en inwerken van nieuwe medewerkers (zowel intern als extern).

In de uitzending van Zembla werd gesteld dat (de top van) de Belastingdienst in maart 2015 gewaarschuwd zou zijn voor een beveiligingslek. Deze bewering is gebaseerd op een document van Liquid Hub van 26 maart 2015. Dit is een presentatie waarin enkele observaties worden gedaan over de positie van een organisatieonderdeel voor activiteiten op het gebied van data-analytics (toen nog onder de titel BIA) en waarin aanbevelingen zijn opgenomen voor de inrichting voor zo'n organisatieonderdeel. Op beveiliging gaat het document niet in, noch bevat dit waarschuwingen over informatiebeveiligingsrisico's. Het document is als bijlage bij deze brief gevoegd[4].

Het huidige niveau van informatiebeveiliging van de afdeling D&A werkt conform het algemene getoetste beveiligingsniveau van de Belastingdienst en kent enkele aanvullende maatregelen. Ik zie daarom op dit moment geen reden tot ingrijpen, maar zoals aangegeven tref ik een aantal nadere maatregelen om de veiligheid nog verder te versterken. De Autoriteit Persoonsgegevens is een onderzoek naar de beveiligingsmaatregelen bij D&A gestart dat op korte termijn ook daadwerkelijk plaatsvindt. Vooralsnog is 13 februari aanstaande afgesproken voor een (eerste) bezoek aan D&A. Indien uit dit onderzoek kwetsbaarheden aan het licht komen, zal ik daarop uiteraard direct passende maatregelen nemen.

### 2. Aanbesteding van de ondersteuning van het programma Broedkamer

Naar aanleiding van de signalen over mogelijke onregelmatigheden bij de aanbesteding van de ondersteuning van het programma Broedkamer, heb ik een extern forensisch onderzoek in gang gezet naar deze aanbestedingsprocedure. Bij het uitzetten van de opdracht wordt er op gelet dat de uitvoerende partij onafhankelijk is ten opzichte van alle deelnemers aan de aanbesteding en niet eerder op enigerlei wijze betrokken is geweest.

In het onderzoek zal onder meer aandacht worden besteed aan de rechtmatigheid en ordelijkheid van de aanbestedingsprocedure zelf, aan mogelijke voorkennis over de opdracht bij de leverancier waaraan de opdracht is gegund en mogelijke banden tussen medewerkers van de Belastingdienst en van de gekozen leverancier. Het onderzoek wordt verricht in opdracht van de directeur-generaal Belastingdienst en ondersteund door een begeleidingscommissie. Mocht uit dit onderzoek blijken dat sprake is van een vermoeden van een strafbaar feit, dan zal daarvan aangifte worden gedaan. De onderzoeker wordt verzocht zijn rapport half mei op te leveren.

Daarnaast zal ik bekijken of, en zo ja hoe de checks en balances in het inkoopproces bij de Belastingdienst verder versterkt kunnen worden. Lopende aanbestedingen worden nauwlettend gevolgd.

### 3. Onderbouwing potentiële baten

In het Algemeen overleg (AO) met uw Kamer op 1 juni 2016 (Kamerstuk 31 066, nr. 295) heb ik potentiële baten van de aanpak van de afdeling D&A genoemd van tussen de € 150 en € 250 mln. Het ging daarbij om niet-gevalideerde inschattingen op basis van geëxtrapoleerde testresultaten van in de Broedkamer ontwikkelde ideeën om de effectiviteit van de

[4] Raadpleegbaar via www.tweedekamer.nl.

handhaving te verbeteren. Deze schattingen kenden dus een ruime onzekerheidsmarge.
Of de potentiële correctieopbrengsten van deze projecten indicatief kunnen zijn voor de baten van de aanpak van de afdeling D&A is onder andere afhankelijk van de wijze van implementatie en toepassing in de praktijk. In het AO van 1 juni heb ik aangegeven dat ik door het ontbreken van een heldere projectplanning ook nog geen goed overkoepelend beeld heb. Dat geldt dus ook voor het ex ante potentieel aan correctieopbrengsten. De bandbreedte van de eerdergenoemde bedragen laten zien dat het om eerste schattingen gaat. Zie ook mijn eedergenoemde brief van 11 oktober 2016 (Kamerstuk 31 066, nr. 304), waarin is aangegeven dat op dat moment een ex ante potentieel aan correctieopbrengst werd verwacht van tussen de € 130 miljoen en € 250 miljoen. De potentiële correctieopbrengsten voor enkele van de D&A-projecten zijn daarin neerwaarts bijgesteld.

Er wordt momenteel gewerkt aan een methodiek voor het meten van de potentiële ex ante baten van de projecten die worden ingezet om de veranderdoelen van de Investeringsagenda te realiseren. Het ex post meten van de bijdrage van de IA-projecten aan de reductie van het nalevingstekort is vrijwel onmogelijk, omdat het resultaat immers ook afhangt van veranderingen in het gedrag van de belastingbetalers en uiteraard gerelateerd is aan de economische ontwikkelingen. De verwachting is dat in de loop van 2017 een methode beschikbaar zal zijn. Ik zal de president van de ARK vragen om een validatie uit te voeren op de ontwikkelde methodiek.

## 4. Managementstijl

De Belastingdienst moet een open en veilige werkcultuur bieden voor zijn medewerkers. Leidinggevenden dienen actief bij te dragen aan het ontstaan en behouden van deze gewenste werkcultuur. Het feit dat betrokkenen verklaringen onder ede afleggen over gevoelde misstanden, wijst erop dat medewerkers onvoldoende hun weg vinden in de lijn, naar meldpunten, integriteitscoördinatoren en vertrouwenspersonen en daarop onvoldoende kunnen vertrouwen. Dit is in lijn met de bevindingen van de Commissie onderzoek Belastingdienst (Cob) op dit punt (Kamerstuk 31 066, nr. 330), die constateert dat de afstand tussen de werkvloer en de top te groot is geworden. Het is een opgave voor het management in de gehele Belastingdienst om de verbinding met de organisatie te herstellen. Een eerste stap is het voeren van het gesprek met de medezeggenschap, om verder zicht te krijgen op wat er speelt. Op basis daarvan zullen ook gesprekken worden gearrangeerd tussen het middle management en medewerkers.

De Belastingdienst was al voornemens in 2017 een medewerkersonderzoek uit te voeren. In het medewerkersonderzoek zullen gerichte vragen worden opgenomen over de werkcultuur in het algemeen en de leidinggevenden in het bijzonder. Zoals gebruikelijk zullen de vragen voorafgaand aan de enquête worden afgestemd met de medezeggenschap. De resultaten en eventuele verbeteracties die daarmee samenhangen zullen eveneens met de medezeggenschap worden besproken.

Verder zal, zoals is aangegeven in de kabinetsreactie op het rapport van de CoB (Kamerstuk 31 066, nr. 330), een ambtelijke topstructuur worden ontworpen die zowel dicht bij de dagelijkse praktijk als bij het ministerie staat. Ook is daarin aangegeven dat het personeelsbeleid, waaronder het beter laten functioneren van vertrouwenspersonen en klokkenluiderregelingen, krachtig ter hand wordt genomen de komende tijd.

**Concluderend**

De uitzending van Zembla bevat ernstige aantijgingen. Die dienen serieus onderzocht te worden. Bij D&A zijn geen acute beveiligingsproblemen, gegeven de analyse van de huidige ICT-beveiliging. Dat laat onverlet dat nader onderzoek naar de periode voor de start van D&A gewenst is.

Zodra het onderzoek van de AP, het eigen onderzoek naar de informatiebeveiliging, het forensisch onderzoek naar de aanbesteding en de validatie van het resultaat van onderzoek naar een meetmethodiek door de ARK gereed zijn, zal ik u hierover informeren. Met de genomen en te nemen maatregelen komt er een extra slot op de deur wat betreft de gegevensbeveiliging en aanbestedingen. Tot slot roep ik de medewerkers op die zich bij Zembla hebben gemeld, om – zodra dat is opgericht – hun informatie, al dan niet anoniem, te delen met het onafhankelijke meldpunt.

De Staatssecretaris van Financiën,
E.D. Wiebes

**Bijlage**

## Aanvullende beveiligingsmaatregelen D&A

Deze bijlage beschrijft een aantal beveiligingsmaatregelen bij D&A aanvullend op het HBB, die mede genomen zijn naar aanleiding van het advies van de ADR. Al getroffen maatregelen zijn:

- Data blijven op één plaats: datasets worden vanuit de bronsystemen ingelezen in een speciale ICT-voorziening voor D&A die zich bevindt in het centrale, hoog beveiligde datacenter van de Belastingdienst in Apeldoorn.
- Door D&A worden geen data uitgeleverd aan andere partijen binnen of buiten de Belastingdienst. Ook aan gebruikers van D&A-producten wordt enkel inkijk geboden.
- Projecten vooraf en in elke volgende fase beoordeeld op gebruik van privacygevoelige gegevens door middel van een Privacy Impact Assessment (PIA).
- Dataclassificatie en compartimentering: data en code wordt ingedeeld in een gevoeligheidsklasse (laag, midden, hoog) en daarop wordt de beveiliging aangepast. Datasets met classificatie «middel», worden extra beveiligd door middel van een extra wachtwoord. Datasets met classificatie «hoog», worden extra beveiligd door deze alleen via een speciale applicatie benaderbaar te maken. Bepaalde persoonsgegevens, zoals nationaliteit en adresgegevens, worden niet in modellen gebruikt vanwege het risico ongeoorloofde discriminatie.
- Vanaf begin 2016 zijn USB-ontheffingen ingetrokken en worden geen nieuwe ontheffingen meer verleend aan medewerkers van D&A.
- Een verplicht te volgen bewustwordingsprogramma voor alle interne en externe medewerkers van D&A, gericht op het verantwoord omgaan met data bij het analyseren van grote datasets.

Lopende initiatieven om de beveiliging nog verder te versterken zijn:

- Ter verdere verhoging van de fysieke toegangsbeveiliging wordt een aanwijzing van de afdeling D&A als «bijzonder werkgebied» ingediend bij de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) vanwege zijn verantwoordelijkheid voor de rijkshuisvesting. Dit houdt in dat aanvullende toegangsbeveiliging wordt ingericht, zodat alleen medewerkers van D&A (en dus niet overige Belastingdienstmedewerkers) de afdeling kunnen betreden. Hiervoor maakt de Belastingdienst op dit moment een risico-inventarisatie. Op grond daarvan wordt de aanvraag door BZK beoordeeld.
- Er wordt een werkwijze geïmplementeerd waarbij identificerende persoonsgegevens worden vervangen door pseudoniemen. Analisten van D&A kunnen persoonsgegevens dan niet meer direct herleiden naar een (rechts)persoon.
- Eind januari is D&A met inzet van experts uit het Security Operations Center (SOC) van de Belastingdienst, gestart met het ontwikkelen van modellen voor extra monitoring. Dat wil zeggen dat modellen worden ontwikkeld voor een geavanceerdere analyse van de loggegevens over het gebruik van applicaties en gegevenssets.
- Dataminimalisatie door verdergaande compartimentering: D&A migreert naar een nieuwe ICT-werkomgeving waarin de medewerkers alleen toegang tot de datasets die zij direct nodig hebben voor hun werk.

**Antwoorden op feitelijke vragen n.a.v. de Zembla-uitzending «Belastingdienst overtreedt willens en wetens privacywet»**

**Vraag 1**
Hoe luidt de contractuele taakopdracht aan Accenture?

**Vraag 2**
Zijn in het contract met Accenture bijzondere voorzieningen opgenomen inzake gegevensbescherming van burgers, met inbegrip van naleving van de fiscale geheimhoudingsplicht, zowel voor het bureau als zodanig als voor de medewerkers die door dit bureau bij de Belastingdienst zijn ingezet? Zo ja, welke voorzieningen zijn getroffen en hoe zijn deze sanctioneerbaar?

**Vraag 3**
Op welke manier wordt Accenture betaalt voor de diensten aan de Belastingdienst? Is er sprake van prestatieafspraken? Wat zijn deze afspraken? Aan welke prestaties is een beloning gekoppeld? Wat voor beloning is aan prestaties gekoppeld? Wie bepaalt of Accenture prestaties haalt? Hoe wordt bepaald of en in hoeverre Accenture prestaties haalt?

**Vraag 4**
Op basis van welke resultaten is Accenture betaald? Hoe werden deze resultaten vastgesteld?

**Antwoord vraag 1 t/m 4**
In verband met de vertrouwelijkheid van contracten met externe partijen beantwoord ik deze vragen niet op deze plek. Op 1 februari jl. heb ik de relevante contracten met Accenture vertrouwelijk naar uw Kamer gestuurd (Aanhangsel Handelingen II 2016/17, nrs. 1048 en 1076). De antwoorden op deze vragen staan in deze contracten. Voor de eisen die zijn gesteld aan externe medewerkers verwijs ik ook naar het antwoord op vraag 5, 57 en 58.

**Vraag 5**
Hoe is, uit een oogpunt van cyberrisico's, het toezicht op de werkzaamheden van de medewerkers van Accenture geregeld?

**Vraag 57**
Op welke punten verschilt de beveiliging die geldt ten aanzien van medewerkers van de Belastingdienst met die van extern ingehuurde partijen, zoals Accenture?

**Vraag 58**
Zijn er waarborgen tegen het risico dat grote bestanden worden gedownload op een USB stick die dan buiten het gebouw terecht komt? Zo ja om welke waarborgen gaat het dan?

**Antwoord vraag 5, 57 en 58**
Toezicht op de werkzaamheden van Accenturemedewerkers vindt plaats doordat ten aanzien van de Accenturemedewerkers de volgende eisen en maatregelen gelden. Deze medewerkers:
a. moeten een geheimhoudingsverklaring ondertekenen;
b. moeten een VOG overleggen aan de Belastingdienst;
c. moeten een Privacy & Security training doorlopen van de Belastingdienst en Accenture;
d. worden gekoppeld aan een interne Belastingdienst medewerker;
e. krijgen alleen toegang tot de gegevens met een Digitale werkplek Belastingdienst (DWB);

f. krijgen geen toegang tot poorten voor gegevensdragers (USB-sticks en dergelijke);
g. krijgen geen toegang tot publieke clouddiensten (bijvoorbeeld: Dropbox en iCloud);
h. krijgen geen mobiel apparaat van de Belastingdienst in bruikleen;
i. mogen de DWB niet meenemen naar huis waardoor alleen binnen de Belastingdienst toegang bestaat tot de gegevens.

Deze maatregelen, met uitzondering van die genoemd onder c (wat betreft de opleiding van Accenture), d, h en i, gelden ook voor Belastingdienst-medewerkers binnen Data en Analytics (D&A). Ten aanzien van maat-regel f kunnen binnen D&A uitsluitend aan Belastingdienstmedewerkers tijdelijke ontheffingen worden verleend voor specifieke werkzaamheden waarvoor zo'n ontheffing nodig is. Hier wordt zeer spaarzaam mee omgegaan en op dit moment zijn die ontheffingen er niet. In het verleden hebben die ontheffingen in ruimere mate bestaan (maximaal 18 met toegang tot data), veelal aan medewerkers die deze ontheffing hadden verkregen vanuit hun vorige functie binnen de Belastingdienst. Eind 2015 zijn deze ontheffingen stapsgewijs ingetrokken op initiatief van de Broedkamer zelf, zodat ultimo 2015, dus voor de oprichting van D&A, alle ontheffingen waren ingetrokken. Sindsdien is nog eenmaal een tijdelijke ontheffing verleend.
Iedere medewerker krijgt tevens een bij de functie behorend autorisatie-profiel. Deze profielen worden centraal binnen de Belastingdienst onderhouden en beheerd. Hierop is binnen D&A actieve logging en monitoring van toepassing, wat betekent dat in elk geval gelogd wordt wie wanneer iets doet, wat iemand doet en welke directories, bestanden en databasetabellen worden gebruikt. Zie hierover ook het antwoord op de vragen 50, 51 en 77.

**Vraag 6**
Klopt het dat we niet weten wie toegang had tot de gegevens in de Broedkamer en wie ze heeft gedownload? Klopt het dat Accenture er toegang tot had? Hoeveel mensen bij Accenture konden bij de gegevens in de Broedkamer? Deelt u de mening dat dit moet worden onderzocht?

**Antwoord vraag 6**
De ICT-infrastructuur van de Belastingdienst voldoet aan alle reguliere informatiebeveiligingseisen die bij de Belastingdienst gelden op grond van het Handboek beveiliging Belastingdienst (HBB). Deze regels zijn voor de gehele Belastingdienst van toepassing en dus ook bij D&A. De periode voorafgaand aan de oprichting van D&A vergt nader onderzoek, zoals aangegeven in de brief waarmee ik deze antwoorden aanbied.
Toegang wordt verleend via autorisaties op persoonsniveau. Het is als gevolg van toepassing van in het Handboek Beveiliging Belastingdienst (HBB) beschreven logging en monitoring bekend wie binnen D&A toegang had tot gegevens. Deze loggegevens zullen worden bekeken, zodat kan worden vastgesteld of getracht is daadwerkelijk gegevens van belastingplichtigen buiten de Belastingdienst te brengen. Het direct downloaden van gegevens uit de D&A-omgeving van databestanden met gegevens van belastingplichtigen buiten die D&A-omgeving is vanaf het begin onmogelijk gemaakt binnen de Broedkamer en D&A, uitgezonderd de in het antwoord op vraag 5, 57 en 58 gegeven USB-ontheffingen. Accenture als bedrijf had geen toegang tot de gegevens. Alleen Accenture-medewerkers die op basis van een contract werkzaam waren binnen de Broedkamer (en later Data&Analytics (D&A)) hadden toegang op basis van specifiek aan hen verleende autorisaties. De Autoriteit Persoonsgegevens (AP) doet onderzoek naar de gegevensbeveiliging bij D&A. Als daaruit blijkt dat nadere maatregelen nodig zijn, zullen die worden getroffen.

**Vraag 7**
Hoe is de verhouding tussen interne en externe medewerkers binnen de Broedkamer? Hoeveel mensen werken er in totaal bij de Broedkamer en hoeveel hiervan zijn extern ingehuurd? Zijn alle externen werkzaam bij Accenture of zijn er nog andere externen werkzaam bij de Broedkamer? Zo ja, van welke organisatie(s)?

**Antwoord vraag 7**
Het contract Intensivering Innovatief Vermogen tussen de Belastingdienst en Accenture is de start geweest van de Broedkamer en heeft een duur gehad van januari 2014 tot en met december 2016. Tot en met medio 2015 zijn er naast Accenture geen externe medewerkers van andere partijen actief geweest. Vanaf de tweede helft van 2015 is het aantal marktpartijen verder uitgebreid op basis van inhuur vallend onder de raamovereenkomsten zoals deze door de Belastingdienst centraal zijn afgesloten. Per begin januari van dit jaar zijn bij D&A externe medewerkers van Accenture, Between (broker), CapGemini, CMotions, GIBBS, Fonkel, ITstaffing (broker), ItaQ, KZA, RiskeMotions en Teradata werkzaam, ieder met hun eigen expertise. Alleen de bij D&A werkzame medewerkers van deze bedrijven hebben toegang tot gegevens onder de voorwaarden zoals genoemd in het antwoord op vraag 5, 57 en 58. Zij hebben geen mogelijkheid om de gegevens buiten de Belastingdienstomgeving te gebruiken. Binnen D&A gelden hiervoor ook geen andere regels dan elders in de Belastingdienst.

In de periode 2014–2016 bestond het aantal medewerkers voor ongeveer 2/3$^{e}$ uit interne medewerkers en 1/3$^{e}$ uit externe medewerkers, met uitzondering van het eerste halfjaar van 2016 (55% intern vs. 45% extern). Door krapte op de arbeidsmarkt en toenemende behoefte aan capaciteit (in zowel ontwikkeling van producten als het beheer ervan) is er gekozen om dit in die periode tijdelijk op te vangen met externe inhuur. Momenteel werken er bij D&A 132 interne medewerkers en 43 externe medewerkers. De doelstelling voor 2017 is om het aantal externe medewerkers verder af te bouwen door overdracht van werkzaamheden aan (deels nieuw te werven) interne medewerkers.

**Vraag 8**
Welke relatie had de toenmalige directeur van de Belastingdienst met Accenture?

**Vraag 9**
Werd de toenmalige directeur van de Belastingdienst betaald voor zijn nevenbezigheden bij Accenture?

**Vraag 12**
In de reportage wordt gesproken van de schijn van belangenverstrengeling met Accenture. Bent u bereid deze verdachtmaking nader te laten onderzoeken?

**Vraag 14**
Is er onderzoek gedaan naar de aanbesteding die Accenture won, zo ja, wat waren de scope en de onderzoeksvraag van dat onderzoek? Zijn er reeds resultaten bekend van dat onderzoek?

**Vraag 15**
Is de aanbesteding van de Broedkamer eerlijk verlopen of heeft Accenture voorinformatie gekregen? Klopt het dat Accenture geholpen is bij het winnen van de aanbesteding?

**Vraag 16**
Zijn de aanbestedingen met onder meer Accenture volgens de wet- en regelgeving verlopen?

**Antwoord vraag 8, 9, 12, 14, 15 en 16**
In de brief waarmee ik deze antwoorden aanbied, heb ik aangekondigd dat een onafhankelijke forensisch onderzoeker de aanbestedingsprocedure zal onderzoeken die heeft geleid tot de opdracht aan Accenture. Daarbij zal ook aandacht worden besteed aan de rol en onafhankelijkheid van medewerkers van de Belastingdienst bij die aanbesteding.

**Vraag 10**
Hadden medewerkers van Accenture in januari 2016 toegang tot hun eigen belastinggegevens? En hadden zij toegang tot de belastinggegevens van bijvoorbeeld hun buurman of hun voormalig partner?

**Vraag 11**
Hoe kan het dat Accenture, zijnde een commercieel bedrijf, toegang had tot alle gegevens?

**Antwoord vraag 10 en 11**
Het bedrijf Accenture heeft nooit toegang gehad tot gegevens van de Belastingdienst. Van Accenture ingehuurde medewerkers hebben binnen de afgeschermde Belastingdienstomgeving toegang tot een selectie van gegevens die nodig zijn voor hun werkzaamheden. Aan het gebruik van deze gegevens zijn strenge eisen gesteld, onder andere om te voorkomen dat deze gegevens gedeeld kunnen worden (zie het antwoord op vraag 5, 57 en 58). Als blijkt dat zij gegevens van een ex-partner of buurman inzien zonder dat het nodig is voor de uitvoering van hun werkzaamheden, worden zij daarop aangesproken, in het licht van naleving van hun geheimhoudingsplicht. Overtreding hiervan kan ultiem via het strafrecht worden gehandhaafd.

**Vraag 13**
Hoe is de aanbesteding gegaan voor de Broedkamer en de investeringsagenda, de aanbesteding die door Accenture is gewonnen? Bent u bereid hier extern onderzoek naar te doen? Waarbij ook gekeken wordt of Accenture voorkennis had bij het schrijven van een offerte?
Klopt het dat het eerde mis is gegaan met aanbestedingsprocedures bij de Belastingdienst? Wat is hiervan geleerd?

**Vraag 17**
Er wordt onderzoek gedaan naar de aanbesteding die Accenture heeft gewonnen, wat wordt er precies onderzocht? Wat is hier de aanleiding voor? Wat zijn de onderzoeksvragen? Wanneer is dit onderzoek gereed? Wie voert dat onderzoek uit?

**Antwoord vraag 13 en 17**
In november 2013 is onder de tien partijen die partij zijn bij een raamovereenkomst met de Belastingdienst voor ICT-adviesdiensten, een offerteverzoek uitgezet voor ondersteuning van de Broedkamer (later D&A). Er zijn zes offertes ontvangen. Op basis van objectieve criteria is de opdracht uiteindelijk aan Accenture gegund. In augustus 2015 is het contract met Accenture aangevuld, in verband met additionele werkzaamheden. De aanbesteding en de aanvulling op het contract zijn begeleid door de inkoopafdeling van de Belastingdienst.
Zoals ik in mijn brief heb aangegeven zal de aanbestedingsprocedure extern forensisch onderzocht worden. In de opdrachtbeschrijving wordt verzocht het onderzoeksrapport half mei op te leveren.

Naar aanleiding van onjuistheden bij eerdere ICT-aanbestedingsprocedures heeft de Belastingdienst in 2016 een proces ingericht om lopende contracten te controleren.[5] Als de aanbestedingsgrens gepasseerd dreigt te worden, dan neemt de Belastingdienst actie. Dit is een continu proces.

**Vraag 18**
Wat is de taakopdracht van de afdeling Data Analytics van de Belastingdienst?

**Vraag 19**
Is het juist dat de werkzaamheden van de Afdeling DataAnalytics het ontwikkelen van data intelligence op basis van Big Data (Datamining) betreft, in het bijzonder gebaseerd op de informatiebevoegdheden van de Belastingdienst in de AWR, de wetgeving inzake de basisregistraties en de sectorwetgeving?

**Vraag 21**
Wat is de grondslag in wet- en regelgeving van de ontwikkeling van data intelligence door de Belastingdienst?

**Antwoord vraag 18, 19 en 21**
De opdracht van D&A is om met bewezen data- en analyticsmethoden en modellen de informatie te leveren die nodig is voor de vormgeving van moderne interactie, voor informatiegestuurd toezicht en informatiegestuurde invordering, alsmede voor sturing, verantwoording en effectmeting, en daarmee een bijdrage te leveren aan het bereiken van de doelen van de Investeringsagenda.
De activiteiten van de afdeling D&A staan direct ten dienste van de uitvoering van de taken van de Belastingdienst, zoals vastgelegd in de artikelen 1 en 3 van de Algemene wet inzake Rijksbelastingen (uitgewerkt in artikel 2 van de Uitvoeringsregeling Belastingdienst), artikel 11 van de Algemene wet inkomensafhankelijke regelingen en de artikelen 1 tot en met 6 van de Invorderingswet 1990. Kort samengevat betreft dit de taken heffen, uitkeren en invorderen; toezicht en handhaving zijn een (belangrijk) onderdeel daarvan. Het betreft publiekrechtelijke taken en wettelijke verplichtingen als bedoeld in artikel 8, onderdelen c en e, van de Wet beschermingpersoonsgegevens, dat daarmee tevens een grondslag biedt om persoonsgegevens te verwerken.
Om deze taken goed te kunnen uitvoeren, beschikt de Belastingdienst (cq. de wettelijk aangewezen functionarissen) over wettelijke bevoegdheden, zowel in fiscale wetgeving en toeslagwetgeving als in sectorwetgeving en basisregistratiewetten, om informatie te verzamelen en te bewerken. D&A werkt niet voor Douane en FIOD.

**Vraag 20**
In hoeverre houden de activiteiten van de Afdeling Data Analytics verband met de ontwikkeling van een Gegevenslandschap, dat wil zeggen de ontwikkeling van een breed toegankelijk Stelsel van persoonsgegevens?

**Antwoord vraag 20**
D&A voert zijn werkzaamheden uitsluitend uit ten behoeve van verbetering van de effectiviteit van toezicht en handhaving door de Belastingdienst. Met de doorontwikkeling van het stelsel van basisregistraties naar een gegevenslandschap voor de overheid houdt dit geen direct verband. De Belastingdienst is wel gebruiker van de basisregistraties en ook van gegevens van andere overheidsorganisaties, die wellicht onderdeel zullen worden van dit landschap. Dat gebruik berust altijd op wettelijke bevoegdheden.

[5] Kamerstuk 34 475 IX, nr. 1, p. 107.

**Vraag 22**
Hebben medewerkers bij de Broedkamer ruimer toegang tot grote databestanden met gegevens over bedrijven en particulieren dan andere werknemers bij de belastingdienst die belast zijn met controle op belastingplichtigen? Waaruit bestaan de verschillen?

**Antwoord vraag 22**
Medewerkers binnen de Belastingdienst hebben alleen maar toegang tot de gegevens die voor hun werk van belang zijn. De wijze van gebruik van die gegevens is ook beperkt tot wat voor de uitoefening van de functie noodzakelijk is. Voor medewerkers van D&A (waar de Broedkamer in op is gegaan), geldt als gevolg daarvan dat zij de belastinggegevens van belastingplichtigen alleen maar kunnen zien en hier analyses op kunnen doen, maar deze niet kunnen wijzigen. Medewerkers die belast zijn met controle op belastingplichtigen, belastingschuldigen en toeslaggerechtigden buiten D&A hebben autorisaties om wijzigingen aan te brengen in diverse primaire informatiesystemen van de Belastingdienst (via applicaties). Deze autorisaties zijn beperkt tot de voor hen relevante gegevens en bestanden. De autorisatie van medewerkers van D&A is in dit opzicht dus beperkter dan van medewerkers die controles uitvoeren.

**Vraag 23**
Hoe hoog is het verloop onder medewerkers die werkzaam zijn bij de Broedkamer?

**Antwoord vraag 23**
Op dit moment werken er in totaal 132 Belastingdienstmedewerkers bij D&A. Begin 2014 waren dit er 44. In 2014 zijn er geen, in 2015 1 en in 2016 5 Belastingdienstmedewerkers uitgestroomd. De instroom van nieuwe Belastingdienstmedewerkers betrof in 2014 20 medewerkers, in 2015 17 en in 2016 57.

**Vraag 24**
Wat is de gemiddelde leeftijd van medewerkers bij de Broedkamer?

**Antwoord vraag 24**
De gemiddelde leeftijd van de Belastingdienstmedewerkers bij D&A (waar de Broedkamer in is opgegaan) is 43 jaar.

**Vraag 25**
Werken er fiscalisten bij de Broedkamer?

**Antwoord vraag 25**
Er werken geen fiscalisten bij de Broedkamer. Er wordt in alle projecten samengewerkt met fiscalisten uit andere onderdelen van de Belastingdienst. Zie ook het antwoord op vraag 29.

**Vraag 26**
Kunt u toelichten of en waarom de Broedkamer gepaard ging met veel geheimzinnigheid? Klopt het dat er ramen werden afgeplakt? Waarom is daarvoor gekozen? Waarom die geheimzinnigheid?

**Antwoord vraag 26**
Ik kan niet nagaan waar deze bewering in Zembla precies betrekking op heeft. Wel weet ik dat in de ontwikkelfase van de Investeringsagenda zogenaamde brown papersessies hebben plaatsgevonden, waarbij ook het afplakken van ramen heeft plaatsgevonden.

**Vraag 27**
Kunt u reageren op de aantijgingen dat er een schrikbewind gevoerd werd bij de Belastingdienst en dan vooral rondom de Broedkamer?

**Vraag 28**
Graag een reactie op het feit dat in de Zembla-uitzending wordt gesproken van malversaties, schrikbewind, manipulatie, etc.?

**Vraag 84**
In hoeverre is en was er sprake van een autocratische top binnen de Belastingdienst?

**Antwoord vraag 27, 28 en 84**
In de brief waarmee ik deze antwoorden aanbied heb ik aangekondigd dat via het medewerkerstevredenheidsonderzoek de werkcultuur in het algemeen en de leidinggevenden in het bijzonder, specifiek aan de orde zullen komen. Dat kan inzicht bieden in de in Zembla geuite zorgen over de wijze van leidinggeven.
Het is van groot belang dat de Belastingdienst haar medewerkers een open en veilige werkcultuur biedt waarin mensen hun zorgen kunnen uiten en signalen serieus worden genomen. Het in te stellen externe meldpunt waar mensen met hun zorgen heen kunnen wanneer zij het gevoel hebben dat ze dit niet bij hun eigen management kwijt kunnen[6], zal hier ook een bijdrage aan leveren. Daarnaast is het van belang om de afstand tussen de top en de werkvloer van de Belastingdienst te verkleinen. In de kabinetsreactie op het rapport van de commissie onderzoek Belastingdienst (Kamerstuk 31 066, nr. 330), is aangegeven dat een ambtelijke topstructuur zal worden ontworpen die zowel dichtbij de dagelijkse praktijk als bij het ministerie staat.

**Vraag 29**
Hoe zijn de medewerkers van de Belastingdienst die niet werkzaam waren in de Broedkamer, betrokken bij de Broedkamer? Kunt u toelichten of u met de kennis van nu, vindt dat medewerkers goed en voldoende betrokken zijn geweest?

**Antwoord vraag 29**
Alle producten van de Broedkamer en D&A worden samen met medewerkers van de Belastingdienst gemaakt. Dat geldt zowel voor het maken van datafundamenten als voor de producten die met behulp van de datafundamenten worden ontwikkeld voor de eindgebruikers in de Belastingdienst. De kennis uit het primaire proces is onder andere nodig om de juiste duiding aan de te gebruiken data te geven. De verantwoordelijken voor het primaire proces beslissen aan In de werkwijze van de Broedkamer en D&A worden gegevens gesorteerd, geïnterpreteerd en van een risicoclassificatie voorzien. Deze risicosignalen gaan via centrale coördinatie naar toezichtmedewerkers. Hiermee wordt mede invulling gegeven aan de wens van de verantwoordelijke directeuren van het primair proces om landelijke centrale regie op de handhavingsstrategie te kunnen vormgeven.
Om de primaire processen te ondersteunen op het gebied van implementatie van de Investeringsagenda, waaronder de producten van de Broedkamer en D&A, is een aparte organisatie ingericht om de implementatie te ondersteunen: de directie Implementatie Ondersteuning. Van daaruitzijn de medewerkers betrokken op het moment dat er een pilot start met een nieuwe innovatie. Deeerste implementaties lopen nu. De opgedane ervaringen bij de ondersteuning van de implementaties worden gebruikt om de implementatiemethode kwalitatief te verbeteren.

[6] Kamerstuk 31 066, nr. 331.

Daarnaast wordt regelmatig op de interne Beeldkrant van de Belastingdienst aandacht besteed aan de ontwikkelingen vanuit de Broedkamer, zodat alle medewerkers geïnformeerd blijven, ook wanneer zij zelf nog niet in hun dagelijkse werk met de nieuwe producten werken. Op deze wijze en anderszins is de Broedkamer en later D&A vele malen onder de aandacht van medewerkers gebracht.
het eind van iedere fase of een project door gaat naar de volgende fase.

**Vraag 30**
Kunt u aangeven of voor alle projecten van de Broedkamer nulmetingen hebben plaatsgevonden? Indien dit niet zo was, voor welke projecten niet?

**Vraag 31**
Graag een reactie op het feit dat in de Zembla-uitzending wordt gemeld dat de prestaties en opbrengsten van de Broedkamer en D&A altijd te positief zijn voorgesteld.

**Vraag 33**
Is er inderdaad gelogen tegen politici, dan wel een onrealistisch positieve versie van de werkelijkheid gepresenteerd? Zijn er inmiddels betrouwbare resultaten van de ingehuurde organisaties?

**Vraag 34**
Klopt het dat de Tweede Kamer verkeerd is voorgelicht over de successen van de Broedkamer, zoals belastingmedewerkers onder ede hebben verklaard?

**Vraag 35**
Kan u reageren op de aantijging dat medewerkers verzocht zijn om politici, bewindspersonen en/of Kamerleden bewust verkeerd te informeren tijdens gesprekken of werkbezoeken?

**Vraag 36**
Hoe zijn medewerkers van de Broedkamer geselecteerd voor het werkbezoek van Kamerleden afgelopen zomer? Zijn zij op enigerlei wijze onder druk gezet om een rooskleuriger presentatie te houden dan zij zelf zouden willen?

**Vraag 37**
Verder horen we dat het bedrag dat de Broedkamer zou opleveren totaal uit de lucht gegrepen is. Klopt dat? Welk bewijs is er dat de Broedkamer honderden miljoenen aan extra belastinginkomsten zou opleveren? Is dat bewijs er wel? Wat is de onderbouwing?

**Antwoord vraag 30, 31, 33, 34, 35, 36 en 37**
In de brief waarmee ik deze antwoorden aanbied, heb ik aangekondigd dat ik de president van de Algemene Rekenkamer (ARK) zal verzoeken om een validatie van een meetmethodiek die ontwikkeld wordt voor verwachte potentiële correctieopbrengsten van de Investeringsagenda. Ik heb uw Kamer hier op 11 oktober over geïnformeerd.[7] In de brief heb ik aangegeven waar ik mij eerder op heb gebaseerd en dat het hierbij gaat om de potentiële (nog te valideren) ex ante baten van de projecten die worden ingezet om de veranderdoelen te realiseren. Het ex post meten van de bijdrage van de IA-projecten aan de reductie van het nalevingtekort is vrijwel onmogelijk, omdat het resultaat immers ook afhangt van de veranderingen in het gedrag van de belastingbetalers en uiteraard ook gerelateerd is aan de economische ontwikkelingen.

[7] Kamerstuk 31 066, nr. 304, bijlage A.

Ik denk niet dat leden van uw Kamer bewust fout zijn voorgelicht tijdens een werkbezoek, maar dat medewerkers op basis van gegevens uit de lab- en pilotfase hun beeld hebben gegeven van de potentiële effecten van de D&A aanpak. Om de ex ante potentiële correctieopbrengsten in te kunnen schatten, wordt een meetmethodiek ontwikkeld. Dat geeft ook uw Kamer meer houvast. De medewerkers die hun zorgen hebben geuit via Zembla, roep ik op zich te melden bij het in te richten meldpunt waar mensen met hun zorgen heen kunnen wanneer zij het gevoel hebben dat ze dit niet bij hun eigen management kwijt kunnen.[8] Op die wijze kunnen de door hen afgegeven signalen worden onderzocht en kan daar waar nodig actie op worden ondernomen.

**Vraag 32**
Welke concrete resultaten zijn tot op heden geboekt door de inzet van de Afdeling Data Analytics?

**Antwoord vraag 32**
In de rapportages over de voortgang van de Investeringsagenda ga ik onder andere in op de resultaten die onder verantwoordelijkheid van de afdeling D&A tot stand komen.

**Vraag 38**
Klopt het dat er sprake is van een beveiligingslek? Indien ja, waarom is dit niet gemeld aan de autoriteit persoonsgegevens? Wanneer bent u op de hoogte gesteld van dit beveiligingslek? Zo nee, waarom was er geen sprake van een beveiligingslek?

**Vraag 39**
Wist u van het lek dat al medio 2015 aan de leiding van de Belastingdienst is gemeld? Waarom is er niks aan gebeurd?

**Vraag 40**
Klopt het dat de Belastingdienst al in 2015 gewaarschuwd is over het gebrek van bescherming van persoonsgegevens binnen de dienst? Door wie is de Belastingdienst allemaal gewaarschuwd over het privacy-lek? Wanneer hebben deze partijen de dienst gewaarschuwd?

**Vraag 41**
Wanneer wist u zelf dat er een probleem was met het privacybeleid en de bescherming van persoonsgegevens?

**Vraag 42**
Is het onderzoek naar een beveiligingslek pas gestart na de uitzending van Zembla? Zo ja, waarom is dit niet eerder gestart? Zo nee, wanneer is het onderzoek dan gestart en zijn er al resultaten? Wanneer kunt u de Kamer informeren over de resultaten van een (al dan niet nog uit te voeren) onderzoek?

**Vraag 44**
Zijn de genoemde beveiligingslekken inmiddels gedicht, en wordt er geïnventariseerd of er verder lekken zijn?

**Vraag 45**
Klopt het dat de ADR concludeert dat de onvoldoende fysieke beveiliging van data een risico vormt voor de vertrouwelijkheid van gegevens en dat maatregelen om dit risico te verhelpen, nog niet zijn geëffectueerd? Kunt u uitleggen wat er gebeurd is met deze conclusies en wanneer dit is

[8] Kamerstuk 31 066, nr. 331.

gedaan? Is op dit moment de fysieke toegangsbeveiliging wel voldoende is? Kunt u dit toelichten?

**Vraag 46**
Waarom is er niets gedaan toen de Belastingdienst op de hoogte was van de onvoldoende beveiliging van de Broedkamer (medio 2015, rapport ADR)?

**Vraag 48**
Waarom golden de strengere beveiligingseisen zoals in het ADR-rapport geformuleerd niet sinds de start van de Broedkamer?

**Antwoord vraag 38, 39, 40, 41, 42, 44, 45, 46 en 48**
Op deze vragen ben ik ingegaan in de brief waarmee ik deze antwoorden aanbied. De AP voert op grond van artikel 60 van de Wet bescherming persoonsgegevens een onderzoek uit naar de beveiliging van de afdeling D&A. Het heeft tot doel vast te stellen in hoeverre de Belastingdienst passende en organisatorische maatregelen heeft getroffen. Op grond van de bevindingen van de AP zullen zo nodig nadere maatregelen worden getroffen. Ik zal uw Kamer informeren over de resultaten. Naar aanleiding van de uitkomsten van het onderzoek van de AP zal ik nader ingaan op deze vragen, voor zover die niet reeds door dat onderzoek worden beantwoord dit onderzoek. Naast het onderzoek van de AP, laat ik zelf de log- en monitorgegevens onderzoeken en de gegevensbeveiliging in de periode voorafgaand aan de oprichting van D&A. Om ook overigens iedere twijfel uit te sluiten, laat ik ook een breed onderzoek uitvoeren op de toepassing van het beveiligingsbeleid bij de Belastingdienst.

**Vraag 43**
Wat voor actie heeft de Belastingdienst of het Ministerie van Financiën ondernomen vanaf het moment dat Zembla vragen heeft gesteld over de beveiliging van persoonsgegevens op de Broedkamer?

**Antwoord vraag 43**
Er heeft vanuit het ministerie overleg plaatsgevonden met D&A en op basis daarvan is opnieuw geverifieerd hoe de gegevensbeveiliging is vormgegeven, welke logging en monitoring plaatsvindt en hoe die is vastgelegd. De gegevensbeveiliging is zodanig dat er geen aanleiding is om te vermoeden dat de beveiliging van (persoons)gegevens bij de afdeling D&A niet voldoet aan de eisen van het HBB. Desondanks neem ik de in Zembla naar voren gekomen signalen serieus. Zoals in de brief opgenomen wordt de gegevensbeveiliging op dit moment verder uitgebreid.

**Vraag 47**
Welke zaken staan er in het ADR-rapport borgingsmaatregelen D&A? Wat is er met dit rapport gedaan? Wat wordt in het ADR-rapport bedoeld met: «Voor beperking van fysieke toegang (zie 3.6 Huisvesting) en nadere inperking van tie logische toegangsbeveiliging om data voor medewerkers af te schermen, zijn gedachten aanwezig zoals toegangspasjes om op tie afdeling te komen, logging en monitoring. Deze maatregelen zijn nog niet geeffectueerd.»

**Antwoord vraag 47**
Op de hoofdlijnen en achtergrond van het rapport en wat er met het betreffende onderzoek is gedaan, ben ik ingegaan in de brief waarmee ik deze antwoorden aanbied. Het onderzoek van de ADR was een eerste, breder onderzoek naar de bedrijfsvoering van D&A, waarvan informatie-

beveiliging een onderdeel uitmaakt. Het ADR-onderzoek is met mijn brief van 28 oktober 2016 aan uw Kamer aangeboden.[9]
Met deze passage licht de ADR toe dat de maatregelen «logging en monitoring» op meerdere gebieden toepasbaar kunnen zijn, zoals fysieke toegang (wie heeft wanneer het pand en/of ruimtes betreden), logische toegang (wie heeft wanneer welke applicaties gebruikt) en datagebruik (wie heeft wanneer welke bestanden gebruikt, gegevens geraadpleegd en/of welke dataverwerkingen uitgevoerd met welk doel).
De ADR heeft aangegeven dat het met de betreffende passage wordt gedoeld op aanwezige plannen om de protectie van datagebruik te verbeteren. De aanduiding dat «deze» maatregelen nog niet zijn geëffectueerd heeft betrekking op de voornemens van de leiding van D&A om aanvullende beveiligingsmaatregelen te treffen naast het toentertijd – ten tijde van de oprichting van D&A als dienstonderdeel – reeds bestaande beveiligingsniveau.

**Vraag 49**
Klopt het dat het niet achterhaald kan worden of de gegevens op dit moment al gekopieerd en gestolen zijn? Kunt u dit toelichten?

**Vraag 67**
Is er daadwerkelijk sprake geweest van een datalek? Waarop is de uitspraak «van verlies en diefstal van gegevens van D&A tot op heden nog niet geconstateerd»? Hoe kan dit worden geconstateerd als er geen sprake is geweest van «logging»? De Zembla-uitzending meldt dat het probleem 2,5 jaar heeft geduurd, klopt dit? Is een eventueel lek gemeld bij de Autoriteit Persoonsgegevens?

**Vraag 78**
Kunt u nagaan of de Wet bescherming persoonsgegevens voldoende is nageleefd bij de Belastingdienst en met name bij de Broedkamer?

**Antwoord vraag 49, 67 en 78**
Er wordt in elk geval gelogd wie wanneer iets doet, wat iemand doet en welke directories, bestanden en databasetabellen worden gebruikt. In de brief heb ik tevens aangegeven dat als extra maatregel de bestaande logginggegevens worden bekeken, zodat kan worden vastgesteld of getracht is daadwerkelijk gegevens van belastingplichtigen buiten de Belastingdienst te brengen. De periode voorafgaand aan de oprichting van D&A (waaronder de Broedkamer) vergt nader onderzoek. Om ook overigens iedere twijfel uit te sluiten, laat ik ook een breed onderzoek uitvoeren op de toepassing van het beveiligingsbeleid bij de Belastingdienst. De AP doet tevens onderzoek naar de beveiligingsmaatregelen bij de Belastingdienst, in het bijzonder D&A, en daarmee naar de naleving van de relevante bepalingen van de Wet bescherming persoonsgegevens.

**Vraag 50**
Hoe zijn de data van belastingbetalers fysiek en digitaal afgeschermd? Wie hebben er bij de belastingdienst, inclusief externen, toegang tot de data van belastingbetalers?

**Vraag 51**
Hoe is de fysieke toegang geregeld bij de Belastingdienst? Wie heeft er toegang tot het gebouw, de gang, de kamer of de locatie met alle gegevens van de belastingbetalers en bedrijven heeft? Hoe wordt dit bijgehouden wie er toegang heeft tot deze locatie?

[9] Bijlage bij Kamerstuk 31 066, nr. 315.

**Vraag 77**
Welke eisen in het kader van privacy en informatiebeveiliging zijn er bij de Belastingdienst of rijksbreed extra voor extern ingehuurde medewerkers ten opzichte van eigen medewerkers?

**Antwoord vraag 50, 51 en 77**
De Belastingdienst beveiligt informatie van belastingplichtigen, belastingschuldigen en toeslaggerechtigden volgens de wettelijke eisen en Rijksbrede kaders die hiervoor gelden, zoals de Wet bescherming persoonsgegevens, het Voorschrift informatiebeveiliging Rijk (VIR), het Normenkader beveiliging Rijkskantoren (NkBR) en de Baseline informatiebeveiliging Rijk (BIR). Voor de Belastingdienst zijn deze eisen en kaders nader uitgewerkt en vastgelegd in het Handboek Beveiliging Belastingdienst (HBB). Zie hierover ook het antwoord op de vragen 70, 71, en 73 tot en met 75. In de brief ben ik ingegaan op verschillende vormen van fysieke en logische gegevensbeveiliging.

Naast de fysieke en logische (digitale) toegangsbeveiliging speelt ook de wettelijke geheimhoudingsplicht van medewerkers een belangrijke rol. Deze vloeit voor de heffing en inning voort uit de Algemene wet inzake rijksbelastingen en de Invorderingswet, en voor uitkering van toeslagen uit de Algemene wet bestuursrecht. Deze geheimhoudingsplicht geldt zowel voor interne als externe medewerkers en blijven ook gelden als medewerkers de dienst hebben verlaten. Voor interne medewerkers geldt bovendien nog de geheimhoudingsplicht op grond van artikel 125a, derde lid, van de Ambtenarenwet. Onder de interne medewerkers vallen ook negen vaste medewerkers van het Ministerie van Financiën die toegang tot het netwerk van de Belastingdienst hebben voor analyses ten behoeve van fiscaal beleid. Voor zover daarbij gebruik wordt gemaakt van de gegevens van D&A via DWB plekken, vallen deze medewerkers onder dezelfde beveiligingsvoorschriften (Handboek Beveiliging Belastingdienst) als de Belastingdienstmedewerkers.
Aan de geheimhoudingsplicht wordt ook aandacht besteed in de Personele uitvoeringsbepalingen Belastingdienst (PUB). Daaruit volgt ook dat een schending van de geheimhoudingsplicht als een ernstige integriteitsschending wordt gezien. In contracten met leveranciers wordt over geheimhouding altijd een artikel opgenomen. Overtreding van geheimhoudingsplicht kan ultiem via het strafrecht worden gehandhaafd. Voorts geldt voor de Belastingdienst de Gedragscode integriteit Rijk, die ook ingaat op veilig en zorgvuldig omgaan met informatie.[10] Deze wordt behandeld tijdens de introductiecursus die verplicht is voor nieuwe interne en externe medewerkers. De Belastingdienst neemt ook deel aan de iBewustzijn Overheid-campagne, waarvan cursussen op het gebied van veilig omgaan met informatie deel uitmaken. Bij de afdeling D&A is deelname aan deze cursus inmiddels verplicht voor zowel interne als externe medewerkers.

**Vraag 52**
Hoe is binnen de Belastingdienst/afdeling Data Analytics voorzien in feitelijke controle op de naleving van de wettelijke regelingen inzake gegevensbescherming, in het bijzonder de Wet bescherming persoonsgegevens c.a. en de AWR?

**Antwoord vraag 52**
Binnen D&A zijn hier drie lijnen voor geïmplementeerd:
1. Alle medewerkers binnen een specifiek project moeten een Privacy en Security bewustwordingscursus volgen en de Tech Lead en Lead Data

[10] Stcrt. 2016, nr. 51732.

Scientist toetsen het data gebruik aan de hand van de aanwijzing Verantwoord Gebruik Data.
2. De Dataprotectiefunctionaris van D&A voert een Privacy Impact Assessment (PIA) uit op elk project. Daarbij wordt hij juridisch ondersteund door de Directie Vaktechniek van de Belastingdienst en het Wbp team van het Directoraat-Generaal Belastingdienst. De Functionaris Gegevensbescherming (FG) van het Ministerie van Financiën houdt toezicht op het hele proces.
3. Externe audits worden verzorgd door de ADR.

**Vraag 53**
Zijn de standaardbeveiligingsmaatregelen voor de Broedkamer sinds 2013 veranderd? Zo ja, wat is er gewijzigd?

**Antwoord vraag 53**
De standaardbeveiligingsmaatregelen zijn veranderd voor zover dit voorvloeide uit jaarlijkse actualisering van het HBB. Het beveiligingsbeleid is in zoverre gewijzigd. Zie daarvoor ook het antwoord op vraag 70,71, 73, 74 en 75.

**Vraag 54**
Hebben medewerkers van de Broedkamer toegang tot hun eigen belastinggegevens (zowel nu als een jaar geleden)? Wordt bijgehouden wanneer medewerkers van de Broedkamer in hun eigen gegevens kijken?

**Antwoord vraag 54**
Medewerkers van de Belastingdienst kunnen, mits zij daartoe geautoriseerd zijn, de voor hen relevante gegevens inzien, waarbij het ook kan gaan om hun eigen belastinggegevens. Dat is voor medewerkers van D&A (waar de Broedkamer in is opgegaan) niet anders. Zij hebben uitsluitend leesrechten en kunnen dus geen gegevens wijzigen. Op basis van de logging en monitoring kan worden gezien welke directories, bestanden en databasetabellen worden gebruikt. Om iedere twijfel uit te sluiten, laat ik een breed onderzoek uitvoeren op de toepassing van het beveiligingsbeleid bij de Belastingdienst.

**Vraag 55**
Indien een medewerker van de Broedkamer (intern of extern) de belastinggegevens bekijkt van bijvoorbeeld zijn voormalige partner, gaat er dan een alarmbel af en wordt de medewerker daarop aangesproken en worden maatregelen genomen?

**Antwoord vraag 55**
Medewerkers van de Belastingdienst (of zij nu werkzaam zijn bij D&A of andere onderdelen van de dienst) hebben de mogelijkheid om gegevens van een voormalige partner in te zien als inzicht in die gegevens voor de uitoefening van de functie noodzakelijk is. Als blijkt dat zij dit doen zonder dat het nodig is voor de uitvoering van hun werkzaamheden, worden zij daarop aangesproken door hun leidinggevende, in het licht van naleving van hun geheimhoudingsplicht.

**Vraag 56**
In hoeverre hebben externen inzicht/inzage in vertrouwelijke persoonsgegevens bij de Belastingdienst en hoe wordt voorkomen dat deze gegevens kunnen uitlekken?

**Antwoord vraag 56**
Extern ingehuurde medewerkers hebben op basis van functie en rol en de op basis daarvan toegekende autorisaties toegang tot dezelfde gegevens als interne collega's in dezelfde functie en rol. Zie voor de eisen en

beperkingen die aan (externe) medewerkers worden gesteld ook het antwoord op vraag 5, 57 en 58.

**Vraag 59**
Welke organisaties en bedrijven hebben (mogelijk) toegang (gehad) tot de data van de Belastingdienst? Wie zijn bijvoorbeeld leverancier en eigenaar van ICTinfrastructuur en ICT-producten? Is de Belastingdienst in staat om deze organisaties te controleren op hoe zij hun toegang gebruiken, en kan de Belastingdienst zonodig zonder deze organisaties functioneren?

**Antwoord vraag 59**
De Belastingdienst is zelf eigenaar van zijn ICT-infrastructuur en ICT-producten. Zowel aanschaf, voortbrenging als beheer en exploitatie zijn bij de IV-organisatie van de Belastingdienst belegd. Hier is dus geen sprake van een uitbestede dienst.
Leveranciers werken nooit zelfstandig binnen het datacenter van de Belastingdienst. Bij bijvoorbeeld onderhoud of storingen werken zij onder begeleiding van Belastingdienstmedewerkers die geautoriseerd zijn voor deze werkzaamheden. Leveranciers van ICT-infrastructuur hebben geen toegang tot data van de Belastingdienst. Aangezien er voor de ICT-infrastructuur continu onderhoud noodzakelijk is zijn er onderhoudscontracten met leveranciers om bijvoorbeeld nieuwe versies van software of beveiligingsupdates te installeren. Om deze reden kan de Belastingdienst niet functioneren zonder deze leveranciers.

**Vraag 60**
Wat voor voorwaarden zijn er gesteld aan de toegang van externen?

**Antwoord vraag 60**
Het is algemeen Belastingdienstbeleid dat externen die door de Belastingdienst zijn ingehuurd alleen toegang krijgen tot gebouwen en systemen op basis van de functie waarvoor zij zijn ingehuurd.

**Vraag 61**
Op welke wijze is er gegarandeerd dat organisaties deze data uitsluitend konden gebruiken voor opdrachten vanuit de Belastingdienst?

**Antwoord vraag 61**
Door beveiligingsmaatregelen als genoemd in het antwoord op vraag 5, 57 en 58 wordt gezorgd dat gegevens alleen voor opdrachten vanuit de Belastingdienst gebruikt kunnen worden.

**Vraag 62**
Wat houden de beveiligingseisen met betrekking tot het loggen en monitoren bij dataverwerking precies in bij zowel de Broedkamer (een jaar geleden), D&A (nu) en de rest van de Belastingdienst?

**Vraag 63**
Klopt het dat er niet bijgehouden wordt via een log wie welke gegevens download? Zo ja, wanneer werd dit bekend? Wat is er meegedaan sinds dit bekend werd? En als het nog niet is opgelost, hoe wordt dit opgelost en op welke termijn?

**Antwoord vraag 62 en 63**
Downloaden van gegevens uit de D&A-omgeving van databestanden met gegevens van belastingplichtigen buiten die D&A-omgeving is niet toegestaan en onmogelijk gemaakt, uitgezonderd de in het antwoord op vraag 5, 57 en 58 gegeven USB-ontheffingen. Zie ook het antwoord op vraag 6. In het HBB staan de voor de gehele Belastingdienst geldende regels rond logging en monitoring. Deze regels zijn niet aangepast in de

periode waarin de Broedkamer is opgestart tot nu. Het HBB en dus ook deze regels gelden voor de gehele Belastingdienst (zie ook het antwoord op de vragen 50, 51, 77 en 70 tot en met 75). Er wordt in elk geval gelogd wie wanneer iets doet, wat iemand doet en welke directories, bestanden en databasetabellen worden gebruikt. Om iedere twijfel uit te sluiten, laat ik een breed onderzoek uitvoeren op de toepassing van het beveiligingsbeleid bij de Belastingdienst.

**Vraag 64**
In hoeverre zijn en waren er autorisatieprofielen en is en was er sprake van logging bij D&A?

**Antwoord vraag 64**
Zie over autorisatie het antwoord op vraag 5 en over logging en monitoring de vragen 62 en 63.

**Vraag 65**
Waarom is bij de Broedkamer niet gelogd wie bij de gegevens kan, wie inlogt en wat ze dan zien of downloaden?

**Antwoord vraag 65**
Toegang tot en het raadplegen van gegevensverzamelingen wordt gelogd. Deze regels worden in de gehele Belastingdienst toegepast en dus ook bij D&A. Het direct downloaden van gegevens uit de D&A-omgeving van databestanden met gegevens van belastingplichtigen buiten die D&A-omgeving is niet mogelijk, uitgezonderd de in het antwoord op vraag 5, 57 en 58 gegeven USB-ontheffingen.

**Vraag 66**
Op welke wijze wordt bij de Belastingdienst en bij de Broedkamer in het bijzonder bijgehouden wie gegevens van belastingplichtigen heeft ingezien?

**Antwoord vraag 66**
Dit wordt geadministreerd via logfaciliteiten. Er wordt in elk geval gelogd wie wanneer iets doet, wat iemand doet en welke directories, bestanden en databasetabellen worden gebruikt. Om iedere twijfel uit te sluiten, laat ik een breed onderzoek uitvoeren op de toepassing van het beveiligingsbeleid bij de Belastingdienst.

**Vraag 68**
Kunt u heel precies aangeven of in januari 2016:
A. wordt bijgehouden wie toegang heeft tot de database van de Broedkamer
B. wie welke data uitleest
C. wie welke data downloadt?

**Antwoord vraag 68**
Ja, deze zaken worden bijgehouden, dus ook in januari 2016. Wie toegang heeft gehad wordt vastgesteld op grond van het gebruikte autorisatieprofiel en vervolgens gelogd. Het direct downloaden van gegevens uit de D&A-omgeving van databestanden met gegevens van belastingplichtigen buiten die D&A-omgeving is niet mogelijk, uitgezonderd de in het antwoord op vraag 5, 57 en 58 gegeven USB-ontheffingen.

**Vraag 69**
Klopt het dat het Ministerie van Financiën eerder verklaarde dat aan alle wet- en regelgeving wordt voldaan bij de Belastingdienst omtrent privacyregels en bescherming? Hoe verhoudt zich dit tot het nieuws wat

Zembla naar buiten bracht dat er grote problemen lijken te zijn rondom de bescherming van persoonsgegevens?

**Antwoord vraag 69**
In de reactie op vragen van het programma Zembla staat dat voor alle afdelingen van de Belastingdienst een streng databeveiligingsbeleid geldt, dat in lijn is met geldende wet- en regelgeving op het terrein van bescherming van (persoons)gegevens, zoals de Wet bescherming persoonsgegevens, het voorschrift informatiebeveiliging Rijksdienst en de internationale richtlijn ISO 27001. Desondanks neem ik de in Zembla naar voren gekomen signalen serieus. Zoals in de brief opgenomen wordt de gegevensbeveiliging op dit moment verder uitgebreid.

**Vraag 70**
Kunt u aangeven wat het officieel vastgestelde databeveiligingsbeleid is dat van toepassing was op de Broedkamer van 2014 tot nu (beleidsbesluit, handboek) was en dat aan de Kamer doen toekomen?

**Vraag 71**
Wat was de vigerende regelgeving voor de beveiliging van de Broedkamer?

**Vraag 73**
Welke wet- en regelgeving is van toepassing op het opslaan en gebruik van gegevens zoals de Belastingdienst heeft?

**Vraag 74**
Aan welke privacyregels moet het omgaan met belastinggegevens voldoen? In hoeverre is hieraan voldaan?

**Vraag 75**
Aan welke eisen moet de informatiebeveiliging van de belastinggegevens volgens de wet- en regelgeving voldoen? Wat is het rijksbeleid of zijn de rijksregels op dit punt? In hoeverre is hieraan voldaan?

**Antwoord vraag 70, 71, 73, 74 en 75**
De Belastingdienst heeft in 2011 het beveiligingsbeleid vastgelegd in het HBB. Dit geldt voor de hele Belastingdienst. Het handboek geeft invulling aan de voor de Belastingdienst toepasselijke wet- en regelgeving op het gebied van bescherming van (persoons)gegevens. Dit zijn in elk geval artikel 13 van de Wet bescherming persoonsgegevens en wettelijke geheimhoudingsplichten (in Awr, Invorderingswet en Awb) en de standaarden NEN/ISO 27001 en NEN/ISO 27002. Deze standaarden zijn voor onderdelen van de rijksdienst uitgewerkt in de Baseline Informatiebeveiliging Rijksdienst (BIR), die is vastgesteld door de Minister van Binnenlandse Zaken en Koninkrijksrelaties.
Het HBB bestaat inmiddels uit vier delen: Deel A, B en C bevatten het strategische, tactische en operationele beveiligingsbeleid en deel D het zogenoemde Business Continity Management. Dit laatste deel is in 2015 toegevoegd en betreft een samenhangend geheel van activiteiten dat er op is gericht de (technische) continuïteit van de organisatie, de veiligheid van medewerkers en bezoekers en de reputatie te borgen.
Het HBB wordt jaarlijks geactualiseerd op basis van wijzigingen in wet- en regelgeving en de genoemde standaarden. Zo zijn de NEN/ISO 27001 en 27002 gewijzigd in 2013. Deze wijziging is uitgebracht in 2014 en verwerkt in het HBB van 2015.
Het HBB is vastgesteld door de leiding van de Belastingdienst en ook de jaarlijkse actualiseringen worden aan de dienstleiding voorgelegd ter beoordeling en goedkeuring.

**Vraag 72**
Wie heeft wanneer gecheckt of er voldaan werd aan de geldende wet- en regelgeving op het gebied van privacy en het beschermen van persoonsgegevens?

**Antwoord vraag 72**
De Belastingdienst voert jaarlijks zelfevaluaties uit op de naleving van het Handboek Beveiliging Belastingdienst. Jaarlijks onderzoekt de Auditdienst Rijk (ADR) een aantal van deze zelfevaluaties. Daarnaast wordt jaarlijks – ingevolge interdepartementale afspraken- door de Secretaris Generaal voor het Ministerie van Financien (inclusief Belastingdienst) een «in control verklaring» (ICV) afgegeven aan de Rijks CIO, waarin bevindingen en risico's worden gerapporteerd op het gebied van informatiebeveiliging.

**Vraag 76**
In hoeverre worden de gebruikte algoritmes onafhankelijk gecontroleerd? Moet dit conform de wet- en regelgeving?

**Antwoord vraag 76**
Ter uitvoering van haar taken genereert D&A op basis van analyse van (persoons)gegevens risicoprofielen voor de selectie van dossiers die voor behandeling in het kader van toezicht in aanmerking komen. Bij de totstandkoming daarvan wordt gebruik gemaakt van door de Belastingdienst aangekochte analysesoftware. Die software maakt gebruik van algoritmes, maar D&A ontwikkelt zelf dus geen algoritmes. De externe softwareleverancier (SAS) laat hun algoritmes beoordelen door het National Institute of Standards and Technology van het Amerikaanse Department of Commerce. Een expliciete verplichting om algoritmen onafhankelijk te laten controleren zit overigens niet in de wet- en regelgeving. In zijn reactie op het rapport «Big Data in een vrije en veilige samenleving» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) (Kamerstukken 26 643 en 32 761, nr. 426) heeft het kabinet aangegeven te onderzoeken hoe, rekening houdend met alle relevante belangen, voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden, met name voor situaties waarin besluitvorming op basis van een Big Data analyse rechtsgevolgen of anderszins een aanmerkelijke impact op burgers heeft. De Belastingdienst is hierbij betrokken.

**Vraag 79**
Erkent u dat de verwerking van gegevens door de Broedkamer de data op grond van de beleidsregels van de Autoriteit Persoonsgegevens gevoeliger maakt?

**Antwoord vraag 79**
De afdeling D&A (en de Broedkamer daarvoor) genereert op basis van analyse van (persoons)gegevens risicoprofielen voor de selectie van dossiers die voor behandeling in het kader van toezicht in aanmerking komen. Dit maakt de gegevens als zodanig niet gevoeliger, maar de toepassing ervan wel. In dit verband stelt artikel 42 van de Wet bescherming persoonsgegevens specifieke eisen aan het gebruik van profilering. Deze zijn uitgewerkt in richtlijnen van de Autoriteit Persoonsgegevens. Het is ook de reden waarom de afdeling D&A inmiddels op een aantal punten strengere beveiligingsmaatregelen heeft genomen dan voortvloeien uit het reguliere beveiligingsbeleid van de Belastingdienst.

**Vraag 80**
Kan het niet ingrijpen na herhaaldelijke signalen over een beveiligingslek of veiligheidsrisico's strafrechtelijke consequenties hebben?

**Antwoord vraag 80**
Nee. Afgezien van een beperkt aantal overtredingen, die samenhangen met het internationale gegevensverkeer, wordt de Wet bescherming persoonsgegevens niet strafrechtelijk, maar bestuursrechtelijk gehandhaafd. Het voor de handhaving bevoegde bestuursorgaan is de AP. Zoals Uw Kamer bekend is, heeft de AP een onderzoek ingesteld naar de beveiliging van de verwerking van persoonsgegevens door de afdeling Data & Analytics van de Belastingdienst. Indien de AP een beveiligingslek heeft vastgesteld kan dit wel leiden tot een bestuurlijke boete van ten hoogste de zesde categorie op grond van artikel 66 tweede lid van de Wet bescherming persoonsgegevens.

**Vraag 81**
Welk onderzoek doet de Autoriteit Persoonsgegevens en wanneer is dit gereed?

**Antwoord vraag 81**
Op 31 januari 2017 heeft de AP de Belastingdienst geïnformeerd een onderzoek in te stellen naar de beveiliging van de verwerking van persoonsgegevens door de afdeling Data & Analytics van de Belastingdienst. Het onderzoek wordt uitgevoerd op basis van de in artikel 60 van de Wet bescherming persoonsgegevens aan de AP toegekende bevoegdheden. Het is mij niet bekend wanneer het onderzoek gereed is.

**Vraag 82**
Welke mensen die genoemd worden in de Zembla uitzending hebben gebruik gemaakt van de «goudgerande» vertrekregeling?

**Vraag 83**
Klopt het dat er een onderzoek naar malversaties door de toenmalige directeur van de Belastingdienst heeft plaatsgevonden? Zo ja, waarom is hier niets over bekend en wat waren de uitkomsten?

**Antwoord vraag 82 en 83**
Ik ga niet in op vragen over individuele ambtenaren.