Reconstructie USB-ontheffingen Belastingdienst

In de onderstaande groene tijdlijn staan de momenten weergeven waarbij vanaf 2017 met de Tweede Kamer is gecorrespondeerd over de USB-ontheffingen. Hierin worden zowel brieven, Kamervragen met antwoorden, nota's, rapporten, rapportages en moties weergegeven. Het onderliggende stuk is onderstreept, vervolgens wordt een beknopte toelichting gegeven. In de blauwe tijdlijn worden de belangrijke interne beleidsstukken weergegeven, in dit geval een handboek en enkele procedures, deze zijn ook onderstreept, met vervolgens een beknopte toelichting.

2017	**8 februari** Brief naar aanleiding uitzending Zembla (Kamerstukken II, 2016/2017, 31 066 nr. 340). Hierin geeft de Staatsecretaris aan dat vanaf begin 2016 alle USB-ontheffingen zijn ingetrokken en geen nieuwe ontheffingen verleend worden aan medewerkers van de directie Data&Analytics (D&A). Daarnaast geeft de Staatssecretaris aan dat binnen D&A uitsluitend aan Belastingdienstmedewerkers tijdelijke ontheffingen worden verleend voor specifieke werkzaamheden waarvoor zo'n ontheffing nodig is. **9 februari** Motie van de leden Omtzigt en Bashir over een extern en onafhankelijk onderzoek naar databeveiliging bij de Belastingdienst (Kamerstukken II, 2016/2017, 31 066 nr. 341). Hierin wordt om een extern en onafhankelijk onderzoek gevraagd naar de databeveiliging bij de Belastingdienst en in het bijzonder de Broedkamer/Data & Analytics vanaf 2013. Deze motie is verworpen. **9 augustus** Rapport van bevindingen onderzoek gegevensgebruik D&A (Kamerstukken II, 2016/2017, 31 066 nr. 379). In het rapport wordt aangegeven dat begin 2017 vijf interne medewerkers over een USB-ontheffing beschikten voor activiteiten rond datalevering. Op 10 januari 2017 is besloten alle USB-ontheffingen in te trekken. Per 26 januari 2017 zijn deze ontheffingen ingetrokken. Op 9 februari 2017 bleek dat één persoon nog over een USB-ontheffing beschikte. Deze is direct ingetrokken. Daarnaast wordt aangegeven dat bij USB-sticks het gebruik wordt gelogd, maar de inhoud van het dataverkeer niet. **21 september** Rapport van bevindingen onderzoek informatiebeveiliging programma Broedkamer en voorlopers (Kamerstukken II, 2016/2017, 31 066 nr. 379). In dit rapport staat aangeven dat gebruik is gemaakt van USB-ontheffingen en dat daarmee sprake was van een risico op het buiten de Belastingdienst brengen van gegevens en oneigenlijk gegevensgebruik. Vervolgens wordt beschreven dat het versleutelen van de gegevens op de USB-device niet

	wordt afgedwongen. Over de periode van het onderzoek (1 januari 2012 t/m 1 februari 2016) zijn er USB-ontheffingen geweest. Deze kwamen over het algemeen mee uit voorgaande functies. Het gebruik van de USB-devices wordt gelogd, alleen de inhoud van het dataverkeer niet. Daarom kon het onderzoek niet vaststellen of gegevens met behulp van USB-devices buiten de Belastingdienst zijn gebracht. **29 november** 20e halfjaars-rapportage. (Kamerstukken II, 2017/2018, 31 066 nr. 380). In deze halfjaars-rapportage wordt teruggekomen op de toezegging om de Kamer te informeren over de technische mogelijkheid om het dataverkeer naar en op USB-sticks te loggen. Aangegeven wordt dat de volgende zaken zijn vastgelegd bij het gebruik van USB-sticks: De medewerkers van de Belastingdienst die geautoriseerd zijn om USB-sticks te gebruiken, de soort autorisatie die zij hebben (lees- en/of schrijfrechten) en voor welke periode. De bestanden die zijn weggeschreven naar USB-sticks, door wie, wanneer en naar welke USB-stick. De mogelijkheid om te loggen welke bestanden zijn weggeschreven bestaat sinds begin oktober 2017. Hierbij worden de bestandsnamen vastgelegd, de inhoud of een hash van het bestand (een unieke code die het bestand identificeert) worden niet vastgelegd. Het lezen van bestanden van USB-sticks wordt niet gelogd. De bestanden op de USB-stick die handmatig zijn ontsleuteld op een Digitale werkplek Belastingdienst (DWB, een beveiligde laptop met de applicaties die de medewerker gebruikt voor zijn werkzaamheden). Dit wordt op dit moment alleen op een DWB zelf geregistreerd. Vanaf begin 2018 wordt dit centraal gelogd. Inmiddels wordt meer gelogd dan alleen het feit dat een USB-stick gebruikt is, zoals nog in het onderzoeksrapport over gegevensgebruik bij D&A werd vermeld. Er worden ook gegevens over het schrijven en ontsleutelen van gegevens op de USB vastgelegd. De Belastingdienst ontwikkelt daarnaast alternatieven voor het gebruik van USB-sticks zoals beveiligde toepassingen voor file transfer en beveiligde samenwerkruimtes, om eventuele risico's bij transport van gegevens zo veel mogelijk te beperken.

2018	**3 juli** Onderzoek AP naar Data & Analytics. (Kamerstukken II 2018/2019, 32 761, nr. 125.) De AP heeft betreffende drie beveiligingsaspecten geconstateerd die niet in orde waren, namelijk:

	"1. Het ontbreken van de logging van de drie activiteiten: export van data vanuit de brongegevens naar de werkplek van een medewerker, het schrijven van data op een USB-stick en het opslaan van bijlagen op mobile devices. 2. De controle op de logging. 3. Het verwijderen/intrekken van autorisaties én te ruime toegangsrechten tot data voor de D&A medewerkers." Vervolgens wordt aangegeven dat het ontbreken van logging van het transporteren van data naar externe gegevensdragers, een risico van de beveiliging van data oplevert. Nergens in de keten wordt vastgelegd door wie, welke data mogelijk onrechtmatig buiten de Belastingdienst wordt gebracht. Achteraf kan ook niet worden nagegaan welke data door wie naar buiten is gebracht. **19 september** Onderzoek naar Belastingdienst, afdeling Data & Analytics. (Kamerstukken I 2017-2018, 32761 125) In dit onderzoek wordt vermeld dat het schrijven van data op een USB-stick binnen DF&A expliciet verboden is. Hierbij wordt alleen in uitzonderlijke gevallen voor beheerders een tijdelijke (lees: enkele uren) autorisatie verleend. Alle verleende tijdelijke USB-ontheffingen zijn vastgelegd in een register. **19 november** Kamervragen m.b.t. logging exporteren data naar USB-sticks (Kamerstukken II, 2018/2019, Aanhangsel 696). In een antwoord op een Kamervraag of er logging plaatsvindt van het exporteren van data naar USB-sticks wordt als antwoord gegeven dat de medewerkers van het dienstonderdeel DF&A die geautoriseerd zijn voor het werken met data niet beschikken over USB-ontheffingen en deze ook niet kunnen verkrijgen. Alleen beheerders van data kunnen een USB-ontheffing aanvragen van enkele uren (dit is het afgelopen jaar (2017) niet gebeurd).

2019	**8 februari** Kamervragen m.b.t. het gebruik USB-sticks (Kamerstukken II, 2018/2019, 32 761 nr. 131). In zijn reactie geeft de Staatsecretaris aan dat het technisch onmogelijk is 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. Daarnaast geeft de Staatssecretaris aan dat een medewerker geautoriseerd kan 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 er 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.

	17 juni Reactie van de Staatssecretaris op Kamervragen (Kamerstukken II, 2018/2019, 32 761 nr. 136). In zijn reactie geeft de Staatsecretaris aan dat binnen DF&A geen enkele medewerker de mogelijkheid heeft om vanaf zijn werkplek gegevens te exporteren naar een USB-stick of een andere externe gegevensdrager. Dit wordt regelmatig gecontroleerd in de autorisatieprofielen. **14 oktober** Onderzoek AP naar Datafundamenten & Analytics (Kamerstukken II 2019/2020, 32 761, nr. 150) In dit onderzoek wordt aangegeven welke constateringen het AP in haar eerste onderzoek heeft gedaan m.b.t. de logging van het exporteren naar externe gegevensdragers. Deze logging ontbrak en daardoor kon niet worden vastgesteld of data buiten de belastingdienst zijn gebracht. Vervolgens wordt er aangegeven dat het risico van de USB-sticks nog verder is beperkt doordat medewerkers geen USB-ontheffing meer krijgen, met uitzondering van beheerders (die daarvoor toestemming moeten vragen bij de verantwoordelijke directeur en de functionaris dataprotectie van DF&A). Deze bij uitzondering verleende autorisaties aan beheerders worden bijgehouden in een logboek en na gebruik direct ingetrokken.

2020	**3 maart** Kamervraag m.b.t. maatregelen DF&A (Kamerstukken II, 2019/2020, 32 761 nr. 159). Als antwoord op een Kamervraag m.b.t. waar medewerkers problemen met de AVG en privacy kunnen melden en hoe daarmee wordt omgegaan geeft de Staatssecretaris als reactie dat binnen DF&A monitoring plaatsvindt op toegekende autorisaties, conflicterende mutatierechten en USB-rechten.

2023	**23 mei** Brief van Staatssecretaris van Financiën (Kamerstukken II, 2022/2023, 31 066 nr. 1236). Nota gebruik USB binnen Belastingdienst. In deze stukken wordt de Kamer geïnformeerd over het beleid rondom het gebruik van USB-sticks binnen de Belastingdienst sinds 2017. In de stukken wordt ingegaan op: • Het huidige beleid ten aanzien van de overdracht van informatie; • De overdracht van gegevens in toezichtprocessen; • De overdracht van gegevens in overige processen; • De overdracht van gegevens in data-analyse bij DF&A; • Het toezicht op de ontheffing voor het gebruik van USB-sticks;

	• Het huidig aantal ontheffingen; • Het onderzoek naar het gebruik van USB-ontheffingen; • De situatie 2017. **5 juli 2023** <u>Eerste stand van zaken Douane.</u> In de stand van zaken geeft de Douane aan dat sinds 2017, toen de Douane nog een directie was binnen de Belastingdienst, geldt dat standaard alle USB-poorten niet gebruikt kunnen worden. Het beleid bij de Douane is dat het gebruik van USB-sticks alleen mogelijk is als er een ontheffing is verleend. Om een ontheffing te krijgen moet de directe leidinggevende toestemming geven. Aanvullend hierop wordt de aanvraag geverifieerd en gecontroleerd door een integrale beveiligingsfunctionaris. De data op de USB-sticks wordt versleuteld en voorzien van een pincode die na een aantal foutieve invoerpogingen het apparaat blokkeert. De gegevens op de USB-stick zijn vervolgens niet leesbaar. **6 juli** <u>Stand van zaken dienst Toeslagen.</u> Ten aanzien van de USB-gegevensdragers bij de Dienst Toeslagen wordt aangeven dat zij gezamenlijk hebben opgetrokken met de Belastingdienst bij het onderzoek over de besluitvorming in 2017 over het USB gebruik, omdat het onderzoek zich met name richt op het beleid van vóór de ontvlechting. Vooruitlopend op dit onderzoek informeert Dienst Toeslagen dat het gebruik van USB-gegevensdragers sterk aan banden is gelegd. In 2017 is een inperking geweest van het aantal uitgegeven USB-autorisaties. Dienst Toeslagen was op dat moment nog onderdeel van de Belastingdienst.

2017	**December** <u>Handboek Beveiliging Belastingdienst (HBB) 2017 Deel B.</u> In het handboek in de algemene Uitvoeringsrichtlijnen staat dat bij fysieke gegevensdragers bedoeld voor gegevensuitwisseling met derden gegevens worden geïsoleerd bijvoorbeeld door middel van encryptie. Bij het informatie uitwisselen met draagbare apparatuur, zoals USB-sticks worden extra beveiligingsmaatregelen getroffen. Hier worden geen onnodig gegevens getransporteerd, worden geen onnodige autorisaties verstrekt en worden hard- en softwarematige voorzieningen aangeboden zoals externe media encryptie. Daarbij wordt kritisch gekeken naar de noodzaak van het gebruik van een bedrijfsmiddel. Het wordt bij voorkeur gekoppeld aan een functie en er wordt op toegezien dat de extra maatregelen ook daadwerkelijk worden gebruikt.

2018	**Mei**

	Procedure Aanvraag van een privilege van Stafdirectie Bedrijfsvoering / Kwaliteitszorg / Informatiebeveiliging. Hierin wordt aangegeven dat begin 2017 alle privileges bij alle medewerkers zijn ingetrokken. Met als richtlijn dat medewerkers die functioneel gebruik moeten maken van een USB-stick en *lees- en schrijfrechten* nodig hebben het privilege moeten aanvragen via hun leidinggevende (in IMS) en dat vooraf door of namens M1 de aanvraag is geaccordeerd. Bij de beoordeling van de aanvraag in IMS dient ook rekening te worden gehouden met nieuwe manieren van dataverplaatsing, zoals Belastingdienst Filetransfer. De manager houdt rekening met de binnen de eigen directie afgestemde werkwijze om te voldoen aan de eis dat voor sommige privileges vooraf (schriftelijk) toestemming door M1 moet plaatsvinden. Ook is besloten om permanent toezicht in te richten op de uitgegeven USB-rechten. In het document staat vervolgens aangegeven wie de doelgroepen zijn voor de USB-ontheffing: 1. EDP-audit specialisten (Lezen en schrijven); 2. Medewerkers controlebureau MKB (Alleen lezen); 3. Controlemedewerkers, inclusief accountants (Alleen lezen); 4. Medewerkers bijzondere teams zoals TRAFI en FEC (lezen en schrijven); 5. Overige aanvragen (Lezen en Lezen & schrijven).

2019	**Mei** Instructie: Toegang tot digitale gegevens (in toezicht). Betreft vertrouwelijk document. Product van Werkgroep toegang tot digitale gegevens (in het toezicht). In deze instructie wordt uiteengezet hoe je op een veilige en verantwoorde manier digitale gegevens van en met belastingplichtigen (en relevante derden) kan uitwisselen. Een uitzonderingssituatie wordt benoemd waarbij de belastingplichtige de gevraagde gegevens niet kan aanleveren op zijn eigen opslagmedium. In die gevallen, mits de medewerker schrijfrechten heeft op de USB-poort, mag een externe gegevensdrager gebruikt worden die de Belastingdienst ter beschikking heeft gesteld. Deze externe gegevensdrager mag nooit onbeheerd ergens achter worden gelaten en de medewerker moet er zelf bij blijven als de belastingplichtige zijn bestanden op de externe gegevensdrager zet. Wanneer een externe gegevensdrager van de Belastingdienst wordt gebruikt, moet die altijd voor en na gebruik geformatteerd worden. Bij het formatteren van een USB-stick is eenmalig volledig formatteren voldoende. Het slechts formatteren met 'quick format' is onvoldoende. Indien het formatteren binnen redelijke termijn niet mogelijk is, kan gekozen worden voor de optie van versleutelen van de ontvangen bestanden met behulp van de DWB. De externe gegevensdrager dient dan op een later tijdstip doch zo spoedig mogelijk alsnog geformatteerd te worden. Daarnaast wordt aangegeven dat het nooit is toegestaan onversleutelde gegevens te vervoeren, dit ter voorkoming van het risico op verlies van gegevens (datalek).